Dr.WEB®

Enterprise Security Suite

Defend what you create

Administrator Manual

© Doctor Web, 2015. All rights reserved

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Enterprise Security Suite
Version 10.0
Administrator Manual
23.11.2015

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1: Welcome to Dr.Web® Enterprise Security Suite 9

1.1. Introduction 9

1.2. Conventions and Abbreviations 10

1.3. About Product 11

1.4. System Requirements 17

1.5. Distribution Kit 21

1.6. Licensing 22

Chapter 2: Components of an Anti-Virus Network and Their Interface 24

2.1. Dr.Web Server 24

2.1.1. Dr.Web Server Management under Windows® OS 25

2.1.2. Dr.Web Server Management under UNIX® System-Based OS 27

2.2. Dr.Web Agent 29

2.3. Dr.Web Security Control Center 30

2.3.1. Administration 33

2.3.2. Anti-Virus Network 34

2.3.3. Neighborhood 39

2.3.4. Search Panel 39

2.3.5. Events 40

2.3.6. Preferences 41

2.3.7. Help 44

2.4. Dr.Web Security Control Center Components 45

2.4.1. Network Scanner 45

2.4.2. License Manager 48

2.5. The Interaction Scheme of an Anti-Virus Network Components 54

Chapter 3: Getting Started. General Information 57

3.1. Establishing a Simple Anti-Virus Network 57

3.2. Setting the Network Connections 58

3.2.1. Direct Connections 59

3.2.2. Dr.Web Server Detection Service 60

3.2.3. Using SRV Protocol 60

Chapter 4: Anti-Virus Network Administrators 61

4.1. Authentication of Administrators 61

4.1.1. Authentication of Administrators from the Server DB 62

4.1.2. Active Directory Authentication 62
4.1.3. LDAP Authentication 63
4.1.4. RADIUS Authentication 64
4.1.5. PAM Authentication 65
4.2. Administrators and Administrative groups 66
4.3. Management of Administrative Accounts and Administrative Groups 68
4.3.1. Creating and Deleting Administrative Accounts and Groups 68
4.3.2. Editing Administrative Accounts and Groups 70
Chapter 5: Groups. Integrated Workstations Management 73
5.1. System and User Groups 73
5.2. Group Management 75
5.2.1. Creating and Deleting Groups 75
5.2.2. Editing Groups 76
5.3. Including Workstations into User Groups 77
5.3.1. Including Stations into Groups Manually 77
5.3.2. Configuring Automatic Group Membership 78
5.4. Using Groups to Configure Stations 80
5.4.1. Inheriting Stations Configuration from Groups. Primary Groups 80
5.4.2. Propagation of Settings to Other Groups/Stations 82
5.5. Comparison of Stations and Groups 82
Chapter 6: Administration of Workstations 83
6.1. Management of Workstation Accounts 83
6.1.1. New Stations Approval Policy 83
6.1.2. Removing and Restoring Stations 84
6.1.3. Merging Stations 85
6.2. General Workstation Settings 86
6.2.1. Station Properties 86
6.2.2. Installed Components of the Anti-Virus Package 89
6.2.3. Hardware and Software on Stations under Windows® OS 90
6.3. Management of Workstation Configuration 91
6.3.1. Permissions of Station Users 91
6.3.2. Scheduled Tasks of a Station 92
6.3.3. Installing Components of the Anti-Virus Package 96
6.4. Management of Anti-virus Components 97
6.4.1. Components 98
6.4.2. Managing Dr.Web Agent for Windows® 100

6.4.3. SpIDer Mail for Windows® Configuration. Application Filter 105
6.5. Anti-Virus Scanning of Stations 106
6.5.1. Viewing and Terminating Running Components 106
6.5.2. Terminating Running Components by Type 107
6.5.3. Launching Scan on Station 107
6.5.4. Configuring Scanner Settings 108
6.6. Viewing Workstation Statistics 114
6.6.1. Statistics 114
6.6.2. Charts 118
6.6.3. Quarantine 119
6.7. Mailing of Installation Files 120
6.8. Sending Notifications to Users 121
Chapter 7: Configuring Dr.Web Server 124
7.1. Logging 124
7.1.1. Audit Log 124
7.1.2. Dr.Web Server Logging 125
7.1.3. Repository Updates Log 126
7.2. Setting Dr.Web Server Configuration 127
7.2.1. General 128
7.2.2. DNS 131
7.2.3. Statistics 132
7.2.4. Security 133
7.2.5. Cache 135
7.2.6. Database 135
7.2.7. Proxy 136
7.2.8. Transport 137
7.2.9. Modules 137
7.2.10. Cluster 138
7.2.11. Location 138
7.2.12. Download 139
7.2.13. Multicast Updates 139
7.2.14. Licenses 140
7.3. Dr.Web Server Remote Access 141
7.4. Setting Dr.Web Server Schedule 141
7.5. Setting the Web Server Configuration 148
7.5.1. General 148

7.5.2. Additional 149
7.5.3. Transport 149
7.5.4. Security 150
7.6. User Hooks 151
7.7. Setting Notifications 153
7.7.1. Notification Configuration 153
7.7.2. Web Console Notifications 157
7.7.3. Unsent Notifications 157
7.8. Administration of Dr.Web Server Repository 158
7.8.1. Repository State 159
7.8.2. Delayed Updates 159
7.8.3. General Repository Configuration 160
7.8.4. Detailed Repository Configuration 162
7.8.5. Repository Content 165
7.9. Additional Features 167
7.9.1. Database Management 167
7.9.2. Dr.Web Server Statistics 169
7.9.3. Backups 170
7.10. Peculiarities of a Network with Several Dr.Web Servers 171
7.10.1. Building a Network with Several Dr.Web Servers 171
7.10.2. Setting Connections between Several Dr.Web Servers 173
7.10.3. Using an Anti-Virus Network with Several Dr.Web Servers 177
7.10.4. Dr.Web Servers Cluster 178
Chapter 8: Updating Dr.Web Enterprise Security Suite Software and Its Components 181
8.1. Updating Dr.Web Server and Restoring from the Backup 181
8.2. Manual Updating of Dr.Web Enterprise Security Suite Components 183
8.3. Scheduled Updates 183
8.4. Updating the Repository of a Server not Connected to the Internet 184
8.4.1. Copying Repository of Other Dr.Web Server 184
8.4.2. Downloading Repository from GUS 185
8.5. Update Restrictions for Workstations 188
8.6. Updating Mobile Dr.Web Agents 189
Chapter 9: Configuring the Additional Components 191
9.1. Proxy Server 191
9.2. NAP Validator 194

Index 197

Chapter 1: Welcome to Dr.Web® Enterprise Security Suite

1.1. Introduction

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator is intended to introduce general features and provide detailed information on the organization of the complex anti-virus protection of corporate computers using **Dr.Web® Enterprise Security Suite**.

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator contains the following parts:

1. **Installation Manual** (the **drweb-esuite-10-install-manual-en.pdf** file)
2. **Administrator Manual** (the **drweb-esuite-10-admin-manual-en.pdf** file)

   Administrator Manual is meant for *anti-virus network administrator* - the employee of organization who is responsible for the anti-virus protection of computers (workstations and servers) of this network

   Anti-virus network administrator should either have a system administrator privileges or work closely with a local network administrator, be competent in anti-virus protection strategy and know in detailes **Dr.Web** anti-virus packages for all operating systems that are used in the network.
3. **Appendices** (the **drweb-esuite-10-appendices-en.pdf** file)

Administrator documentation contains cross-references between three mentioned documents. If you download these documents to the local computer, cross-references work only if documents are located in the same folder and have their initial names.

Administrator documentation does not include the description of **Dr.Web** anti-virus packages for protected computers. For relevant information, please consult **User Manuals** of **Dr.Web** anti-virus solution for corresponding operating system.

Before reading these document make sure you have the latest version of the Manuals. The Manuals are constantly updated and the current version can always be found at the official web site of **Doctor Web** at http://download.drweb.com/esuite/.

1.2. Conventions and Abbreviations

Conventions

The following conventions are used in the Manual.

Table 1-1. Conventions

Symbol	Comment
Note, that	Marks important notes or instructions.
Warning	Warns about possible errors.
Dr.Web Scanner	Names of **Dr.Web** products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples, input to the command line and application output.
Appendix A	Cross-references or Internal Hyperlinks to web pages.

Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

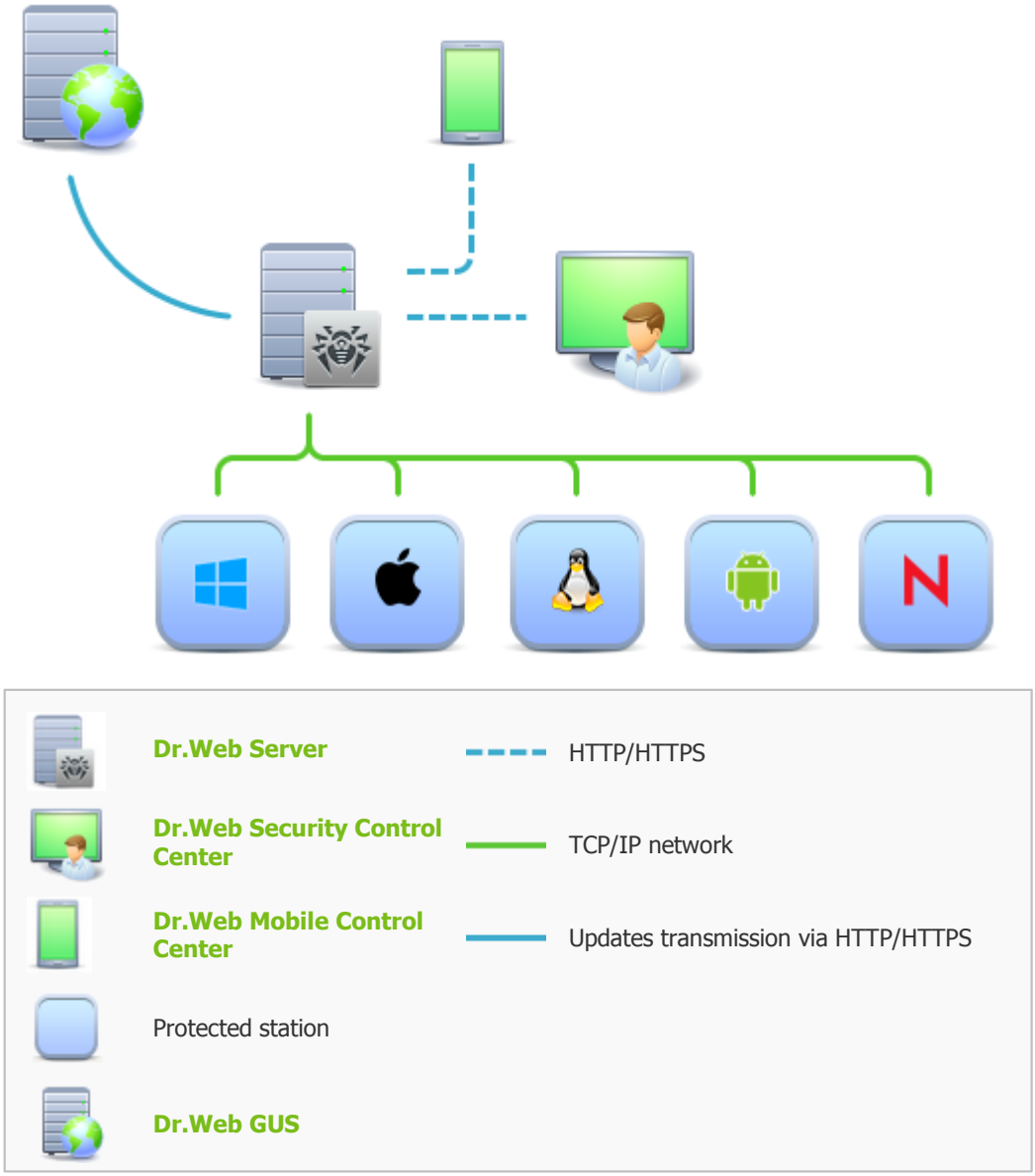
- ACL – Access Control List,
- CDN – Content Delivery Anti-virus network,
- DB, DBMS – Database, Database Management System,
- DFS – Distributed File System,
- DNS – Domain Name System,
- **Dr.Web GUS** – **Dr.Web Global Update System**,
- EBNF – Extended Backus-Naur Form,
- GUI – Graphical User Interface, a GUI version of a program – a version using a GUI,
- LAN – Local Area Network,
- MTU – Maximum Transmission Unit,
- NAP – Network Access Protection,
- OS – operating system,
- PC – personal computer,
- TTL – Time To Live,
- UDS – UNIX domain socket.

1.3. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either local company network including mobile devices, or home computers of employers.

An aggregate of computers and mobile devices on which **Dr.Web Enterprise Security Suite** cooperating components are installed, represents a single *anti-virus network*.

Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on a computers and mobile devises of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP network protocols. Anti-virus software can be installed (and manage them afterwards) on protected stations either via the LAN, or via the Internet.



The logical structure of the anti-virus network

Central Protection Server

Central protection **Server** is installed on a computer of anti-virus network, and installation can be performed on any computer, not only on that functioning as a LAN server. General requirements to this computer are given in the System Requirements section.

Cross-platform **Server** software allows to use a computer under the following operating systems as a **Server**:

- Windows® OS,
- UNIX® system-based OS (Linux®, FreeBSD®, Solaris™).

Central protection **Server** stores distribution kits of anti-virus packages for different OS of protected computers, updates of virus databases and anti-virus packages, license keys and package settings of protected computers. **Server** receives updates of anti-virus protection components and virus databases via the Internet from the **Global Update System** and propagate updates on protected stations.

Hierarchical structure of several Servers can be established to serve protected stations of anti-virus network.

Server supports the backup of critical data (databases, configuration files, etc.).

Server writes single log of anti-virus network events.

Single Database

The single database is connected to the central protection **Server** and stores statistic data on anti-virus network events, settings of the **Server** itself, parameters of protected stations and anti-virus components, installed on protected stations.

You can use the following types of databases:

Embedded database. Two variants of database that is inbuilt into the central protection **Server** directly are provided:

- SQLite2 (InitDB),
- SQLite3.

External database. Inbuilt drivers for connecting the following databases are provided:

- Oracle,
- PostgreSQL,
- ODBC driver to connect other databases such as Microsoft SQL Server/Microsoft SQL Server Express.

You can use any database that corresponds to your demands. Your choice should be based on the needs that must be satisfied by the data store, such as: capability to service the anti-virus network of corresponding size, features of database software maintenance, administration capabilities provided by the database itself and also requirements and standards which are accepted for use in your company.

Central Protection Control Center

Central protection **Control Center** is automatically installed with the **Server** and provides the web interface for remote managing of the **Server** and the anti-virus network by means of editing the settings of the **Server** and protected computers settings stored on the **Server** and protected computers.

The **Control Center** can be opened on any computer that have the network access to the **Server**. The **Control Center** can be used almost under any operating system with full use on the following web browsers:

- Windows® Internet Explorer®,
- Mozilla® Firefox®,

- Google Chrome®.

The list of possible variants of use is given in the System Requirements section.

Central protection **Control Center** provides the following features:

- Serviceability of **Anti-virus** installation on protected stations including: remote installation on protected stations under Windows OS with preliminary browsing the network to search computers; Creation of distribution files with unique identifiers and parameters of connection to the **Server** to facilitate **Anti-virus** installation process by the administrator or possibility of **Anti-virus** installation by users on stations by oneself .
- Facilitate administering based on grouping of anti-virus network workstations (detailed information see in the Chapter 5: Groups. Integrated Workstations Management section).
- Feasibility of centralized administrating of stations anti-virus packages including: uninstallation either separate components or entire **Anti-virus** on stations under Windows OS; configuring parameters of anti-virus package components; assigning permissions to set up and administer the anti-virus packages on protected computers for users of these computers (detailed information see in the Chapter 6: Administration of Workstations section).
- Centralized administering of workstations anti-virus check including: remote launch of anti-virus check either according the specified schedule or direct request from administrator for the **Control Center**; centralized configuration of check parameters and transmitting them to the workstations to launch the local check with these parameters (detailed information see in the Anti-Virus Scanning of Stations section).
- Receiving the statistic information on protected stations states, viral statistics, installed anti-virus software state, running anti-virus components state and also, the list of hardware and software on protected station (detailed information see in the Viewing Workstation Statistics section).
- Flexible administrating system of **Server** and anti-virus network based on opportunity of permissions delimiting for different administrators and also, possibility to connect administrators via the external authorization systems such as Active Directory, LDAP, RADIUS, PAM (detailed information see in the Chapter 4: Anti-Virus Network Administrators section).
- Managing the licensing of workstations anti-virus protection with branched system of assigning licenses to stations, groups of stations and also, granting licenses between several **Servers** in multiserver configuration of anti-virus network (detailed information see in the License Manager section).
- Wide set of setting to configure the **Server** and its separate components including: configuring schedule to maintain the **Server**; plug in user hooks; flexible configuration of update system of all anti-virus network components from the **GUS** and further propagation of updates on stations; configuring the system of administrator notifications about anti-virus network events with different methods of notification delivering; configuring neighbor connections to configure multiserver anti-virus network (detailed information see in the Chapter 7: Configuring Dr.Web Server section).

Detailed information on features for installation of anti-virus protection on workstations is given in the **Installation Manual**.

The par of the **Control Center** is the **Web server** that is automatically installed with the **Server**. The general task of the **Web server** is performing operation with web pages of the **Control Center** and clients network connections.

Central Protection Mobile Control Center

As a separate component, the **Mobile Control Center** is provided. It is designed for installation and operation on mobile devices under iOS and Android OS. General requirements to the application are given in the System Requirements section.

Mobile Control Center connects to the **Server** according to the anti-virus network administrator credentials including via an encrypted protocol. **Mobile Control Center** supports the base set of **Control Center** functions:

1. Manage **Dr.Web Server** repository:
   - view the products state in the repository;
   - launch repository update from **Dr.Web Global Update System**.
2. Manage stations on which an update of anti-virus software is failed:
   - display failed stations;
   - update components on failed stations.
3. Display statistics information on anti-virus network state:
   - number of stations registered at **Dr.Web Server** and their current state (online/offline);
   - viral statistics for protected stations.
4. Manage new stations waiting for connection to **Dr.Web Server**:
   - approve access;
   - reject stations.
5. Manage anti-virus components installed on anti-virus network stations:
   - launch the fast or full scan either for selected stations or for all stations of selected groups;
   - setup **Dr.Web Scanner** reaction on malware detection;
   - view and manage files in the **Quarantine** either for selected stations or for all stations in the selected group.
6. Manage stations and groups:
   - view properties;
   - view and manage components composition of anti-virus package;
   - delete;
   - send custom messages to stations;
   - reboot stations under Windows OS;
   - add to favorites list for the quick assess.
7. Search for stations and groups in an anti-virus network by different parameters: name, address, ID.
8. View and manage messages on major events in an anti-virus network via the interactive Push notifications:
   - display all notifications at **Dr.Web Server**;
   - set reactions on notification events;
   - search notification by specified filter parameters;
   - delete notifications;
   - exclude notifications from automatic deletion.

You can download **Mobile Control Center** from the **Control Center** or directly in App Store and Google Play.

Network Stations Protection

On protected computers and mobile devices of the network, the control module (**Agent**) and the anti-virus package for corresponding operating system are installed.

Cross-platform software allows to provide anti-virus protection of computers and mobile devises under the following operating systems:

- Windows® OS,
- UNIX® system-based OS,
- OS X®,
- Android OS,
- Novell® NetWare® OS.

Either user computers or LAN servers can be protected stations. Particularly, anti-virus protection of the Microsoft® Outlook® mail system is supported.

Control module performs regular updates of anti-virus components and virus databases from the **Server** and also, sends information on virus evens on protected computer to the **Server**.

If the central protection **Server** is not accessible, it is possible to update virus databases on protected stations via the Internet from the **Global Update System**.

Depending on the operating system of the station, the following protection functions are provided:

Stations under Windows® OS

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** including rootkits check is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Mail monitor

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is is also available (if the license permits this function).

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office control

Controls access to network and local resources, in particular, limits access to web sites. Allows to control the integrity of important files from the accidental change or virus infecting and limit the access to unwanted information for employees.

Firewall

Protects computers from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Self-protection

Protects files and folders of **Dr.Web Enterprise Security Suite** from unauthorized or accidental removal and modification by user or malicious software. If self-protection is enabled, access to files and folders of **Dr.Web Enterprise Security Suite** is granted to **Dr.Web** processes only.

Preventive protection

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocks them in case of detection of viral activity.

Stations under UNIX® system-based OS

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Stations under OS X®

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Mobile devices under Android OS

Anti-virus check

Scans a mobile device on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. The check of all files as they are saved in the memory of the device.

Calls and SMS Filter

Filtering the incoming phone calls and SMS allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detect the device location or lock its functions in case it has been lost or stolen.

Restricting Internet Access

URL filter allows to protect user of the mobile device from unsolicited Internet sites.

Firewall

Protects the mobile device from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Security Troubleshooting

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

Application launch control

Blocks the launch on mobile device those applications that are not included into the list of allowed by administrator.

Servers under Novell® NetWare® OS

Anti-virus check

Scans a computer on user demand and according to the schedule.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Providing a Connection between Anti-virus Network Components

To provide stable and secure connection between anti-virus network components, the following features are presented:

Dr.Web Proxy server

Proxy server can optionally be included into the anti-virus network. The main function of the **Proxy server** is to provide connection between the **Server** and protected stations in cases when direct connection is impossible. E.g. if the **Server** and protected stations are located in different networks which do not have packet routing between them. At the expense of using caching function, reducing of network traffic and time of receiving updates by protected stations can be provided.

Traffic compression

Special compression algorithms are applicable for transferring data between the anti-virus network components to reduced network traffic to minimum.

Traffic encryption

Data transferred between the anti-virus network components can be encrypted to provide additional secure level.

Additional Features

NAP Validator

NAP Validator is provided as a separate component and allows to use Microsoft Network Access Protection (NAP) technology to check health of protected stations software. The resulting security is achieved through the implementation of the requirements for performance of network stations.

Repository loader

Dr.Web Repository loader is provided as a separate utility and allows to download products of **Dr.Web Enterprise Security Suite** from the **Global Update System**. It can be used for downloading of **Dr.Web Enterprise Security Suite** products updates to place them on the **Server** not connected to the Internet.

1.4. System Requirements

For Dr.Web Enterprise Security Suite to be installed and function the following is required:

- **Dr.Web Server** should be installed on a computer that have an access to the Internet to receive updates from **Dr.Web GUS** (Global Update System) automatically;

It is allowed to propagate updates by any other way to the **Servers** which are not connected to the Internet. Particularly, in multiserver configuration of anti-virus network, it is possible to receive updates from the **GUS** by only one **Server** with subsequent distribution to other **Servers**, or to use **Dr.Web Repository Loader** additional utility to download updates from the **GUS** with subsequent distribution to **Servers**.

- anti-virus network computers should have access to **Dr.Web Sever** or to the **Proxy server**;

- for interaction between the anti-virus components, the following ports must be opened on used computers:

Port numbers	Protocols	Connection directions	Purpose
2193	TCP	• incoming, outgoing for the **Server** and **Proxy server** • outgoing for the **Agent**	For connection between the **Server** and anti-virus components and for interserver communications. Also is used by **Proxy server** to establish a connection with clients.
	UDP	incoming, outgoing	For the **Network Scanner**.
139, 445	TCP	• incoming for the **Server** • incoming, outgoing for the **Agent** • outgoing for the computer on which the **Control Center** is opened	For the **Network Installer**.
	UDP	incoming, outgoing	
9080	HTTP	• incoming for the **Server** • outgoing for the computer on which the **Control Center** is opened	For **Dr.Web Security Control Center**.
9081	HTTPS		
10101	TCP		For **Server** remote diagnostic utility.
80	HTTP	outgoing	For receiving updates from **GUS**.
443	HTTPS		

The 2371 port is required for connection (via TCP and UDP protocols) between components of **4.XX** version. It is used for support of compatibility, particularly during upgrade of anti-virus network components.

Dr.Web Server requires:

Component	Requirement
CPU and operating system	The following operating systems installed on a computer with corresponding CPU are supported: ◆ CPU that supports SSE2 instructions and has 1,3 GHz or faster clock frequency: • Windows; • Linux; • FreeBSD; • Solaris x86. ◆ V9 UltraSPARC IIIi CPU or later: • Solaris Sparc. Complete list of supported OS see in the **Appendices** document, in Appendix A.
RAM	• Minimal requirements: 1 GB. • Recommended requirements: 2 GB and more.
Free disk space	Up to 12 GB: up to 8 GB for a embedded database (installation catalog) and up to 4GB for the system temporary catalog (for work files). Depending on the **Server** settings, additional space may required to store temporary files, e.g. to store personal installation packages of **Agents** (app. 8,5 MB for each) in the `var\installers-cache` subfolder of **Dr.Web Server** installation folder.

Component	Requirement
	To install the **Server**, it is required on Windows OS system disk or in the `/var/tmp` for UNIX system-based OS (or in the other temporary files folder, if it is redefined), not dependently on the **Server** installation folder, at least 1,2 GB for the general distribution kit and 2,5 GB for the extra distribution kit of free system disk space to launch the installer and unpack temporary files.
Other	For the installation of **Dr.Web Server** for UNIX system-based OS, the following libraries required: `lsb` v. `3` or later, `glibc` v. `2.7` and later. To use **PostgreSQL** DB, the `libpq` required. To use **Oracle** DB, the `libaio` required. Additionally under **FreeBSD** OS, the `compat-8x` library required.

Dr.Web Proxy Server requires:

Component	Requirement
CPU	Intel® Pentium® III 667 MHz or faster
RAM	not less than 1 GB.
Free disk space	not less than 1 GB.
Operating system	• Windows; • Linux; • FreeBSD; • Solaris. Complete list of supported OS see in the **Appendices** document, in Appendix A.
Other	For the installation of **Proxy Server** for UNIX system-based OS: `lsb` v. `3` or later. Additionally under **FreeBSD** OS, the `compat-8x` library required.

Dr.Web Security Control Center requires:

- Windows Internet Explorer 8 and later, Mozilla Firefox 25 and later or Google Chrome 30 and later web browsers.

Opera® 10 and later, Safari® 4 and later web browsers also can be used. But operating under these web browsers is not guaranteed.

Full operability of the **Control Center** under Windows Internet Explorer 8 web browser with the *Enhanced Security Configuration for Windows Internet Explorer* mode enabled is not guaranteed.

If you install **Server** on a computer with a '_' (underline) character in the name, configuration of **Server** with **Dr.Web Security Control Center** by use of Windows Internet Explorer will not be available.

In this case, use other web browser.

For proper operation of **Control Center** in Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed **Dr.Web Server** must be added to the trusted sites of browser, on which you open **Control Center**.

For proper opening of **Control Center** via the **Start** menu in Microsoft Internet Explorer browser under Windows 8 and Windows Server 2012 OS with tiled interface, set the following parameters of a web browser: **Tools** → **Programs** → **Opening Internet Explorer** set the **Always in Internet Explorer** flag.

- **Dr.Web Security Control Center** extension to use **Dr.Web Security Control Center** in full. The extension is distributed with the **Server** installation package. It installs by browser request when you use elements of **Dr.Web Security Control Center** which require the extension (for instance, for anti-virus components remote updater or **Network Scanner**). The extension can be installed on Windows Internet Explorer 8 and later or Mozilla Firefox 25 and later web browsers.

For operation of **Dr.Web Security Control Center** extension at the **Network Scanner** page, under both Windows and GNU/Linux OS, you must have administrator (root) rights.

Under Mozilla Firefox web browser, **Dr.Web Security Control Center** extension is available under Windows OS and Linux system-based OS only.

- Recommended screen resolution to use **Dr.Web Security Control Center** is 1280x1024 pt.

Dr.Web Mobile Control Center requires:

Requirements are differ depending on the operating system on which the application is installed:

- iOS:

Component	Requirement
Operating system	iOS® 7 and later
Device	Apple® iPhone® Apple® iPad®

- Android OS:

Component	Requirement
Operating system	Android 4.0 and later

The NAP requires:

For Server

- Windows Server® 2008 OS.

For the Agents

- Windows XP SP3 OS, Windows Vista OS, Windows Server 2008 OS.

Dr.Web Agent and the full anti-virus package require:

Requirements are differ depending on the operating system on which anti-virus solution is installed (the full list of supported OS see in the Appendix A. The Complete List of Supported OS Versions):

- Windows OS:

Component	Requirement
CPU	1 GHz CPU or faster.
Free RAM	Not less than 512 MB.
Free disk space	1 GB for executable files + extra disk space for logs and temporary files.
Other	1. **Dr.Web Agent for Windows** context help requires Windows® Internet Explorer® 6.0 or later. 2. For **Dr.Web for Outlook** extension the the Microsoft Outlook client from the Microsoft Office package is required: ◆ Outlook 2000 (Outlook 9),

Component	Requirement
	◆ Outlook 2002 (Outlook 10 or Outlook XP), ◆ Office Outlook 2003 (Outlook 11), ◆ Office Outlook 2007 (Outlook 12), ◆ Office Outlook 2010 (Outlook 14), ◆ Office Outlook 2013 (Outlook 15).

- Linux system-based OS:

Component	Requirement
CPU	32-bit (IA-32, x86) and 64-bit (x86-64, x64, amd64) Intel platforms.
Free RAM	Not less than 512 MB.
Free disk space	Not less than 400 MB of free disk space on a volume on which **Anti-virus** folders are placed.

- OS X: configuration requirements coincide with the requirements for operating system;
- Android OS: configuration requirements coincide with the requirements for operating system;
- Novell NetWare OS: configuration requirements coincide with the requirements for operating system.

No other anti-virus software (including other versions of **Dr.Web** anti-virus programs) should be installed on the workstations of an anti-virus network managed by **Dr.Web Enterprise Security Suite**.

Functionality of **Agents** is described in the user manuals for corresponding OS.

1.5. Distribution Kit

The program software is distributed depending on the OS of the selected Dr.Web Server:

1. For UNIX system-base OS - as `run` files for installation under corresponding OS versions of the following components:
   - **Dr.Web Server** general distribution kit,
   - **Dr.Web Server** extra distribution kit,
   - **Proxy Server**.
2. For Windows OS - as installation wizard executable files for installation of the following components:
   - **Dr.Web Server** general distribution kit,
   - **Dr.Web Server** extra distribution kit,
   - **Proxy Server**,
   - **Dr.Web Agent** for Active Directory,
   - Utility for Active Directory scheme modification,
   - Utility to change attributes for Active Directory objects,
   - **NAP Validator**.

Dr.Web Server distribution kit contains two packages:

1. *General distribution kit* - basic distribution kit to install **Dr.Web Server**. Composition is similar to composition of previous versions of **Dr.Web Enterprise Security Suite** distribution.

General distribution kit performs the installation of **Dr.Web Server** itself and includes anti-virus protection packages for stations under Windows OS only.

2. *Extra distribution kit* - includes distributions of all enterprise products, which are provided for installation on protected stations under all supported OS.

   The package is installed as an additional on a computer with **Dr.Web Server** *general distribution kit* installed.

Extra distribution kit must be installed from the same type of package as a general distribution kit.

Dr.Web Server general distribution kit contains the following components:

- **Dr.Web Server** software for the respective OS,
- **Dr.Web Agents** software and anti-virus packages software for supported OSs,
- **Dr.Web Security Control Center** software,
- Virus databases,
- **Dr.Web Security Control Center** extension,
- **Dr.Web Server FrontDoor** extension,
- Manuals, templates, and examples.

In addition to the distribution kit, serial numbers are also supplied. Having registered these serial numbers one can get files with a **Server** key and an **Agent** key.

1.6. Licensing

Rights to use **Dr.Web Enterprise Security Suite** are regulated by the license key file.

Key files have a write-protected format based on the mechanism of electronic signature. Editing the file makes it invalid. Therefore it is not recommended to open your key file with a text editor, which may occasionally corrupt it.

Dr.Web Enterprise Security Suite license parameters and price depend on the number of protected computers, which includes the servers protected by **Dr.Web Enterprise Security Suite** network.

Before purchasing a license for a **Dr.Web Enterprise Security Suite** solution you should carefully consider this information and discuss all the details with your local distributor. The number of **Dr.Web Servers** running the network does not affect the license price.

Licensing specific and key files management for already deployed anti-virus network are described in details in p. License Manager.

When purchasing a license for **Dr.Web Enterprise Security Suite** anti-virus, you receive registration keys or a registration card with a serial number.

License key files are generally sent to users by e-mail, after the product serial number has been registered at the special web site: http://buy.drweb.com/register/ unless otherwise specified in the registration card attached to the product. Visit the web site above, in the form enter your personal data and in the corresponding field type the registration serial number (it is written on the registration card). An archive with key files will be sent to the designated address. Or you will be allowed to download it directly from the web site.

As a rule, key files come in a zip-archive, which contains key files for the **Server** and for workstations.

Users can receive key files in one of the following ways:

- by e-mail (usually after registration of the serial number at the web site, see above);
- with the anti-virus distribution kit if license files were included at kitting;
- as a file on a separate carrier.

Please keep key files until they expire. They are required during the installation and re-installation of the anti-virus, as well as to restore program components. In case a license key file is lost, you need to complete the registration form at the web site specified above so that you can restore it. Note that you will need to enter the same registration serial number and the same personal data as during the first registration, you can change the e-mail address only. In this case the license key file will be sent to the new address.

To try the **Dr.Web Enterprise Security Suite** anti-virus and familiarize yourself with the software, you can order demo keys. Such key files provide for the full functionality of the main anti-virus components, but have a limited term of use. Demo key files are sent upon request made through the web form at https://download.drweb.com/demoreq/biz/. Your request for demo keys will be examined and, if approved, an archive with key files will be sent to the designated address.

The use of obtained key files during the installation is described in **Installation Manual**, p. Installing Dr.Web Server.

Chapter 2: Components of an Anti-Virus Network and Their Interface

2.1. Dr.Web Server

An anti-virus network built with **Dr.Web Enterprise Security Suite** must have at least one **Dr.Web Server**.

To increase the reliability and productivity of an anti-virus network and distribute the computational load properly, **Dr.Web Enterprise Security Suite** anti-virus can also be used in the multiserver mode. In this case the **Server** software is installed on several computers.

Dr.Web Server is a memory-resident component. **Dr.Web Server** software is developed for various OS (see the Appendices document, p. Appendix A).

Basic Functions

Dr.Web Server performs the following tasks:

- initializes of installation of the **Agent** software and anti-virus packages on a selected computer or a group of computers;
- requests the version number of the anti-virus package and the creation dates and version numbers of the virus databases on all protected computers;
- updates the content of the centralized installation folder and the updates folder;
- updates virus databases and executable files of the anti-virus packages, as well as executable files of the program on protected computers.

Collecting Information on Anti-Virus Network

Communicating with **Dr.Web Agents**, **Dr.Web Server** collects and logs information on operation of the anti-virus packages. Information is logged in the general log file implemented as a database. In small networks (not more than 200-300 computers) an embedded database can be used. In larger networks it is recommended to use an external database.

An embedded DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Dr.Web Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.

Otherwise, you must use an external DB.

If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:

- 3 GHz processor CPU,
- RAM at least 4 Gb for **Dr.Web Server** and at least 8 Gb for the DB server,
- UNIX system-based OS.

The following information is collected and stored in the general log file:

- versions of the anti-virus packages on protected computers,
- time and date of the software installation and update on workstations,
- versions and dates of virus databases updates,

- OS versions of protected computers, processor type, OS system catalogs location, etc.,
- configuration and settings of anti-virus packages,
- data on virus events, including names of detected viruses, detection dates, actions, results of curing, etc.

Dr.Web Server notifies the administrator on virus events occurring on protected computers by e-mail or through the Windows OS standard broadcast notification system. You can set the alerts as described in p. Setting Alerts.

Web Server

Web server is a part of **Dr.Web Security Control Center** and performs the following general functions:

- authentication and authorization of administrators in the **Control Center**;
- automation of **Control Center** pages operation;
- support for dynamically generated pages of **Control Center**;
- support for HTTPS-protected client connections.

2.1.1. Dr.Web Server Management under Windows® OS

Interface and Dr.Web Server Management

Dr.Web Server has no interface. As a rule, **Dr.Web Server** can be managed via **Dr.Web Security Control Center** which acts as an interface for the **Server**.

Elements to facilitate adjusting and managing the **Server** are placed by the installation wizard in the **Programs** main Windows OS menu, the **Dr.Web Server** folder:

- The **Server control** folder in its turn contains the commands to start, restart and shut down the **Server**, as well as the commands to set up the logging parameters and other **Server** commands described in detail in the **Appendices** document, p. H3. Dr.Web Server.
- **Web interface** item opens **Dr.Web Security Control Center** and connects to the **Server** installed at this computer (at the http://localhost:9080).
- **Documentation** item opens administrator documentation in HTML format.

Dr.Web Server installation folder has the following structure:

- `bin` – **Dr.Web Server** executable files.
- `etc` – general configuration files of anti-virus network components.
- `Installer` – program to install the **Anti-virus** on a protected computer and the public encryption key file (`drwcsd.pub`).
- `update-db` – scripts necessary to update the structure of **Server** DB.
- `var` – contains the following subfolders:
  - `es-dl-cache` – customers' personal installation packages during two weeks after their creation.
  - `backup` – backups of DB and other critical data.
  - `extensions` – scripts of user hooks meant to automate the performance of certain tasks.
  - `repository` – repository folder to store actual updates of virus bases, anti-virus packages files and anti-virus network components. It contains subfolders for the program components software which include subfolders for their versions depending on the OS. The folder should be accessible for writing to the user under which the **Server** is launched (the **LocalSystem** as a rule).
  - `templates` – a set of reports templates.

- `webmin` – **Dr.Web Security Control Center** elements: documents, icons, modules.

The content of the updates catalog `\var\repository` is automatically downloaded from the updates server through HTTP\HTTPS protocol according to the **Server** schedule, or the anti-virus network administrator can manually place the updates to the catalog.

General Configuration Files

File	Description	Default folder
`agent.key` (name may vary)	**Agent** license key	`etc`
`certificate.pem`	SSL certificate	
`download.conf`	network settings for generating of the **Agent** installation packages	
`drwcsd.conf` (name may vary)	**Server** configuration file	
`drwcsd.conf.distr`	**Server** configuration file template with default parameters	
`drwcsd.pri`	private encryption key	
`enterprise.key` (name may vary)	**Server** license key file. The file is saved if it presented after the upgrade from the previous versions. For the new **Server 10.0** installation, the file is absent	
`frontdoor.conf`	configuration file for the **Server** remote diagnostic utility	
`http-alerter-certs.pem`	certificates for verification the apple-notify.drweb.com host for sending push notifications.	
`private-key.pem`	RSA private key	
`webmin.conf`	**Control Center** configuration file	
`auth-ads.xml`	configuration file for administrators external authorization via Active Directory	
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP	
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS	
`database.sqlite`	embedded database	`var`
`drwcsd.pub`	public encryption key	• `Installer` • `webmin\install`

Start and Stop Dr.Web Server

By default, **Dr.Web Server** automatically starts after installation and every time after restarting the operating system.

Also you can start or start, restart or stop **Dr.Web Server** by one of the following ways:

For Windows OS

- General case:
  - Using the corresponding command, located in the **Start** → **Programs** → **Dr.Web Server** menu.
  - Via the services management tools in the **Administrative Tools** section at the **Control Panel** of Windows OS.

- Stop and restart via the **Control Center**:
  - In the **Administration** section, use buttons: to restart, to stop.
- Using the console commands run from the `bin` subfolder of the **Server** installation folder (see also the **Appendices** document, p. H3. Dr.Web Server):
  - `drwcsd start` – start the **Server**.
  - `drwcsd restart` – total restart of the **Server** service.
  - `drwcsd stop` – normal shutdown of the **Server**.

Please note, if you need the **Server** to read environment variables, the service must be rebooted via the services management tools or via the console command.

2.1.2. Dr.Web Server Management under UNIX® System-Based OS

Interface and Dr.Web Server Management

Dr.Web Server has no interface. As a rule, **Dr.Web Server** can be managed via **Dr.Web Security Control Center** which acts as an interface for the **Server**.

Dr.Web Server installation folder has the following structure:

`/opt/drwcs/` for Linux and Solaris OS and `/usr/local/drwcs` for FreeBSD OS:

- `bin` – **Dr.Web Server** executable files.
- `doc` – license agreements files.
- `ds-modules`
- `fonts` – fonts for **Control Center** interface.
- `Installer` – network installer and the public encryption key file to install the **Anti-virus** on a protected computers.
- `lib` – libraries set for **Server** operation.
- `update-db` – scripts necessary to update the structure of **Server** DB.
- `webmin` – **Dr.Web Security Control Center** elements.

`/var/opt/drwcs/` for Linux and Solaris OS and `/var/drwcs` for FreeBSD OS:

- `backup` – backups of DB and other critical data.
- `bases` – unpacked virus bases for backward compatibility with previous versions of **Dr.Web Agents**.
- `coredump` – **Server** crash dumps.
- `database.sqlite` – **Server** embedded database.
- `etc` – general configuration files of anti-virus network components.
- `extensions` – scripts of user hooks meant to automate the performance of certain tasks.
- `installers-cache` – **Agent** installers cache. Meant to store **Agent** installation packages when stations are created via the **Control Center**.
- `log` – **Server** log files.
- `object` – **Control Center** objects cache.
- `reports` – temporary folder for generating and storing reports.
- `repository` – repository folder to store actual updates of virus bases, anti-virus packages files and anti-virus network components. It contains subfolders for the program components software which include subfolders for their versions depending on the OS. The folder should be accessible for writing to the user under which the **Server** is launched (the **drwcs** as a rule).

- `run` – **Server** process PID.
- `sessions` – **Control Center** sessions.
- `upload` – folder to download temporary files which are specified via the **Control Center** (keys, etc.).

`/etc/opt/drweb.com/` for Linux OS (only for installation from `*.tar.gz.run` generic packages) and `/usr/local/etc/opt/` for FreeBSD OS:

- `software/drweb-esuite.remove` – script to remove the **Server**.
- + possible extra files and folders.

`/usr/local/etc/rc.d/` for FreeBSD OS:

- `drwcsd.sh` – script to start and stop the **Server**.

`/var/tmp/drwcs` – backup after **Server** removal.

General Configuration Files

File	Description	Default folder
`agent.key` (name may vary)	**Agent** license key	• for Linux OS and Solaris OS: /var/opt/drwcs/etc • for FreeBSD OS: /var/drwcs/etc
`certificate.pem`	SSL certificate	
`common.conf`	configuration file (for some of UNIX system-based OS)	
`download.conf`	network settings for generating of the **Agent** installation packages	
`drwcsd.conf` (name may vary)	**Server** configuration file	
`drwcsd.conf.distr`	**Server** configuration file template with default parameters	
`drwcsd.pri`	private encryption key	
`enterprise.key` (name may vary)	**Server** license key file. The file is saved if it presented after the upgrade from the previous versions. For the new **Server 10.0** installation, the file is absent	
`frontdoor.conf`	configuration file for the **Server** remote diagnostic utility	
`http-alerter-certs.pem`	certificates for verification the apple-notify.drweb.com host for sending push notifications	
`private-key.pem`	RSA private key	
`webmin.conf`	**Control Center** configuration file	
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP	
`auth-pam.xml`	configuration file for administrators external authorization via PAM	
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS	
`database.sqlite`	embedded database	• for Linux OS and Solaris OS: /var/opt/drwcs

File	Description	Default folder
		• for FreeBSD OS: /var/drwcs
drwcsd.pub	public encryption key	• for Linux OS and Solaris OS: /opt/drwcs/Installer /opt/drwcs/webmin/install • for FreeBSD OS: /usr/local/drwcs/Installer /usr/local/drwcs/webmin/install

Start and Stop Dr.Web Server

By default, **Dr.Web Server** automatically starts after installation and every time after restarting the operating system.

Also you can start or start, restart or stop **Dr.Web Server** by one of the following ways:

For UNIX system-based OS

- Stop and restart via the **Control Center**:
  - In the **Administration** section, use buttons: to restart, to stop (is absent under Solaris OS).
- Using the corresponding console command (see also the **Appendices** document, p. H3. Dr.Web Server):
  - Start:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh start
      ```
    - for Linux OS and Solaris OS:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Restart:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh restart
      ```
    - for Linux OS and Solaris OS:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - Stop:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh stop
      ```
    - For Linux OS and Solaris OS:
      ```
      # /etc/init.d/drwcsd stop
      ```

Please note, if you need the **Server** to read environment variables, the service must be rebooted via the console command.

2.2. Dr.Web Agent

Detailed description of **Agent** and its operation principals you can find in the **Dr.Web® Agent for Windows. User manual**.

Principle of Operation

Workstations are protected from virus threats by **Dr.Web** anti-virus packages designed for correspondent OS.

The packages operate by **Dr.Web Agents**, which is installed and constantly resided in the memory of protected workstations. They maintain connection to **Dr.Web Server**, thus enabling administrators to centralized configure anti-virus packages on workstations from **Dr.Web Security Control Center**, schedule anti-virus checks, see the statistics of anti-virus components operation and other information, start and stop remotely anti-virus scanning, etc.

Dr.Web Servers opportunely download updates and distribute them to the **Agents** connected to them. Thus due to **Dr.Web Agents** anti-virus protection is implemented, maintained and adjusted automatically, without user intervention and irregardless of user's computer skills.

In case an anti-virus station is outside the anti-virus network, **Dr.Web Agent** uses the local copy of the settings and the anti-virus protection on that computer retains its functionality (up to the expiry of the user's license), but virus databases and program files are not updated.

Updating of mobile **Agents** is described in p. Updating Mobile Agents.

Basic Functions

Dr.Web Agent is designed to perform the following:

- installs, updates and sets up the anti-virus package, starts scans, and performs other tasks given by **Dr.Web Server**;
- allows to call for execution the **Dr.Web** anti-virus package files through a special interface;
- sends the results of tasks execution to **Dr.Web Server**;
- sends notifications of predefined events in the operation of the anti-virus package to **Dr.Web Server**.

Every **Dr.Web Agent** is connected to **Dr.Web Server** and is included in one or several groups registered on this **Server** (for more, see p. System and User Groups). The **Agent** and **Dr.Web Server** communicate through the protocol used in the local network (TCP/IP of 4 or 6 version).

Hereinafter a computer on which **Dr.Web Agent** is installed as per its functions in the anti-virus network will be called a *workstation*, while in the local network it can be functioning both as a server or a workstation.

2.3. Dr.Web Security Control Center

To manage the anti-virus network and set up the **Server**, the in-built **Dr.Web Security Control Center** serves.

For correct functioning of **Dr.Web Security Control Center** under Windows Internet Explorer browser, you must add **Dr.Web Security Control Center** address to the list of trusted sites in the web browser settings: **Tools** → **Internet Options** → **Security** → **Trusted Sites**.

For correct functioning of **Dr.Web Security Control Center** under Chrome browser, you should turn on cookies.

Connecting to Dr.Web Server

From any computer with network access to the **Server**, **Dr.Web Security Control Center** is available at the following address:

`http://`*<Server_Address>*`:9080`

or

`https://`*<Server_Address>*`:9081`

where *<Server_Address>* is the IP address or domain name for the computer on which **Dr.Web Server** is installed.

Ports numbers for HTTP connection and for protected HTTPS connection are differ: `9080` and `9081` correspondingly.

In the authorization dialog window specify the user name and password of the administrator (by default, administrator name is **admin** and the password is the same, as was specified during **Server** installation).

If you connect through HTTPS protocol (secure SSL connection), the browser requests you to approve the **Server** certificate. Warnings and indications of distrust to the certificate may display, because the certificate is unknown to your browser. You need to approve the certificate to connect to **Dr.Web Security Control Center**.

Some browsers, e.g. **FireFox 3** and later report errors when connecting through HTTPS and refuse connection to **Dr.Web Security Control Center**. To solve this problem, add **Dr.Web Security Control Center** to the list of exceptions by clicking **Add site** in the warning message. This allows connection to **Dr.Web Security Control Center**.

Dr.Web Security Control Center Interface

Dr.Web Security Control Center window (see figure 2-1) is divided in *main menu header* and *working area*.

Working Area

The working area is used to perform all the main functions of **Dr.Web Security Control Center**. It consists of two or three panels depending on the actions which are being performed. Items in the panels are nested from left to right:

- the *control menu* is always located in the left part of the working area,
- depending on the selected item, one or two additional panels are displayed. In the latter case, the rightmost panel contains the settings of elements from the central panel.

The interface language must be set individually for each administrator account (see p. Managing Administrator Accounts).

Main menu

The main menu consists of the following items:

- Administration section,
- Anti-virus network section,

- Neighborhood section,
- Search panel,
- the name of the current administrator logged into **Dr.Web Security Control Center**. Also, the interserver connections menu may be available.
- Events section,
- Preferences section,
- Help section,
- **Logout** to close the current **Dr.Web Security Control Center** session.

If automatic authorization in **Control Center** is enabled, after clicking **Logout**, information about administrator's login and password is deleted.

At next logon in the **Control Center**, it is necessary to repeat standard authorization procedure with specifying login and password. If automatic authorization is enabled, specified login and password are saved for the current web browser and authorization in **Control Center** become automatic (without login and password confirmation) till next **Logout** clicking.

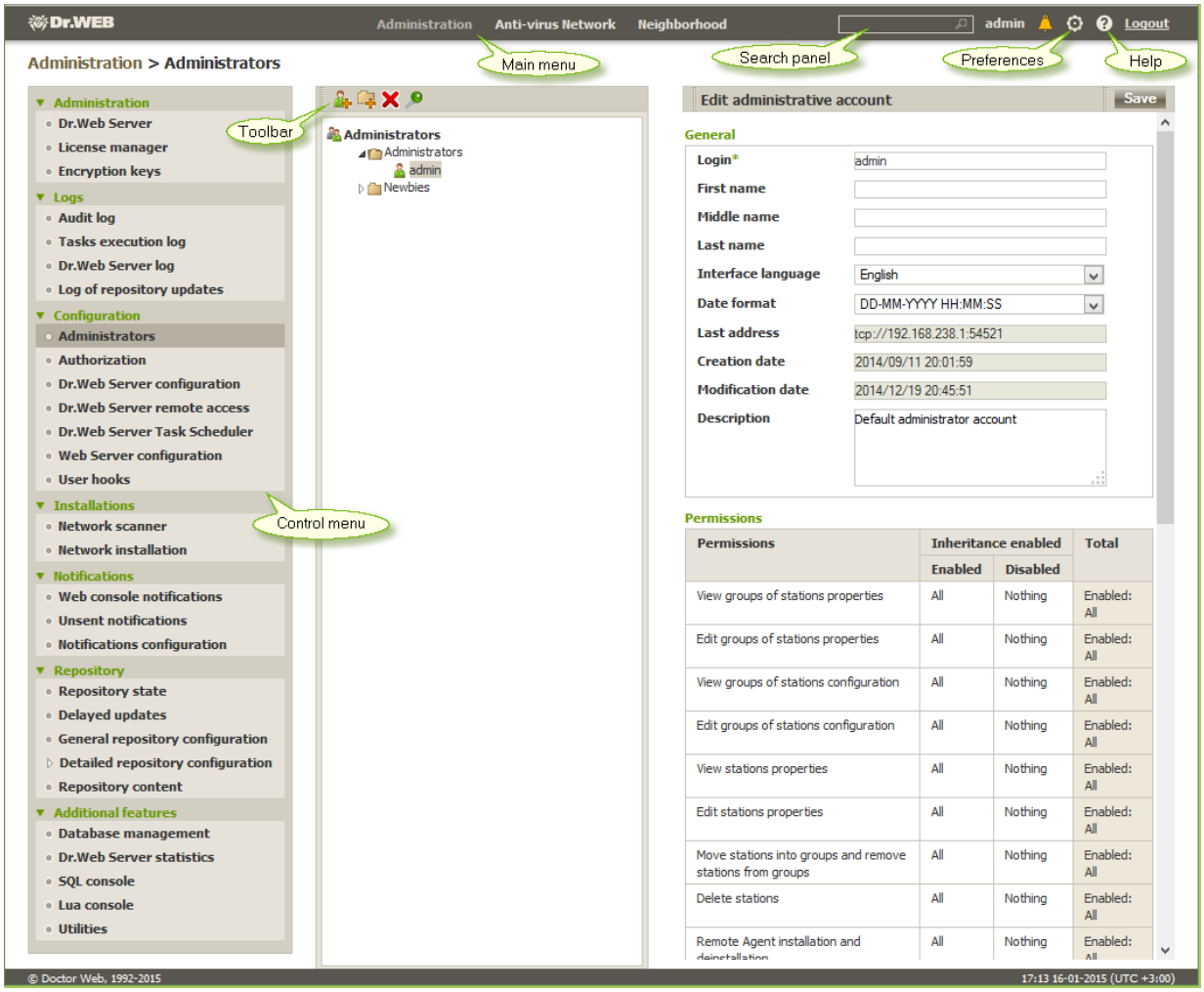


Figure 2-1. Dr.Web Security Control Center window. Click the main menu option to see the description

Interserver Connections Menu

Information on multiserver anti-virus networking and configuring neighbors is given in the Peculiarities of a Network with Several Dr.Web Servers section.

If interserver connections with other **Dr.Web Servers** are configured, the following functions are added to the administrator login on the main menu:

- Next to the administrator login, the name of current **Dr.Web Server** is shown.
- Clicking on administrator login opens drop-down list with connected neighbor **Servers**. If the name for a neighbor is not specified, its identifier is given.
  On neighbor click, two options are possible:
  - The **Control Center** of neighbor **Server** opens if the IP address of the **Control Center** was specified during connection configuring.
    The action is similar to the button on the toolbar in the **Neighbors** section on the main menu.
  - If the **Control Center** address of this neighbor **Server** is not set, the setting of the **Neighbors** section opens to specify the IP address.

2.3.1. Administration

Select the **Administration** item in the main menu of **Dr.Web Security Control Center**. The control menu in the left part of the window is used to view and edit information in the opened window.

The control menu consists of the following items:

1. **Administration**
   - **Dr.Web Server** – opens the panel which shows basic information about the **Server** and lets you restart or shutdown it via the and (is absent under Solaris OS) buttons in the top right part of the panel. Also if **Dr.Web Server** has updates downloaded, from this section you can access the Dr.Web Server Updates section with the **Server** versions list to update and back up.
   - License Manager – allows to manage the license key files.
   - **Encryption keys** – allows to export (save locally) public and primary encryption keys.
2. **Logs**
   - Audit log – allows to view the list of events and changes carried via the control subsystems of **Dr.Web Enterprise Security Suite**.
   - **Tasks execution log** – contains the list of **Server** tasks with completion marks and comments.
   - Dr.Web Server log – contains the list of events on the **Server** operation.
   - Log of repository updates – contains the list of updates from **GUS**, that includes detailed information on updated products revisions.
3. **Configuration**
   - Administrators – opens the panel for managing anti-virus network administrator accounts.
   - Authentication – opens the panel to manage authentication methods of **Dr.Web Security Control Center** administrators (see Authentication of Administrators).
   - Dr.Web Server configuration – opens the panel with main settings of the **Server**.
   - Dr.Web Server remote access – contains settings for connecting **Server** remote diagnostics utility.
   - Dr.Web Server Task Scheduler – opens the panel with **Server** task scheduler settings.
   - Web server configuration – opens the panel with general settings of the **Web server**.
   - User hooks.
4. **Installations**
   - Network Scanner – allows to specify a list of networks, search for installed anti-virus software in networks to determine protection status of computers, and install anti-virus software.
   - **Network installation** – allows to simplify installation of the **Agent** software on certain workstations (see **Installation Manual**, p. Installing Dr.Web Agent Software via Dr.Web Security Control Center).

5. **Notifications**
   - Web console notifications – allows to view and manage administrator notifications which are received via the **Web console** method.
   - Unsent notifications – allows to track and manage administrative notifications failed to be sent according to the settings of the **Notification Configuration** section.
   - Notifications configuration – allows to configure administrative notifications on anti-virus network events.
6. **Repository**
   - Repository state – allows to check repository state: date of last update of repository components and their state.
   - Delayed updates – contains the list of products that are temporary disabled for updating in the **Detailed repository configuration** section.
   - General repository configuration – opens the window to configure settings of connection to the **GUS** and repository updates for all products.
   - Detailed repository configuration – allows to setup revisions configuration for each repository product separately.
   - Repository content – allows to view and manage current repository content as files and folders of repository folder.
7. **Additional features**
   - Database management – allows direct maintenance of **Dr.Web Server** database.
   - Dr.Web Server statistics – contains statistics of this **Server** operating.
   - **SQL console** – allows to execute SQL queries to the database which **Dr.Web Server** uses.
   - **Lua console** – allows to execute LUA scripts both typed in the console directly or loaded from a file.
   - **Utilities** – opens the section with additional utilities for interaction with **Dr.Web Enterprise Security Suite**:
     - Dr.Web Repository Loader to download **Dr.Web Enterprise Security Suite** products from the **Global Update System**.
     - **Dr.Web Server remote diagnostics utility** allows remotely connect to **Dr.Web Server** for basic controlling and viewing the operation statistics. Graphical version of the utility is available for Windows OS only. See also Dr.Web Server Remote Access.
     - **Dr.Web Mobile Control Center** for administrating the anti-virus network based on **Dr.Web Enterprise Security Suite**. Designed for installation and operation on mobile devices under iOS and Android OS.

2.3.2. Anti-Virus Network

Select the **Anti-virus network** item in the main menu of **Dr.Web Security Control Center**.

Control Menu

To view and edit the information in the opened window, use the control menu resided in the left part of the window.

Control Menu contains the following components:

1. **General**
   - Charts
   - Running components
   - Installed components
   - Quarantine

- Comparison of hardware and software (when a group or several stations are selected)
- **User sessions**
- **Inactive stations**
- Hardware and software (when stations are selected)
- Properties
- Group membership rules (when user groups are selected)

2. Statistics
3. **Configuration**
   - Permissions
   - Task Scheduler
   - Installing components
   - Update Restrictions
   - The list of anti-virus components for operating system of selected station or by list of operating systems when a group is selected.

The list of anti-virus component settings and setup recommendations are listed in the **User Manual** for corresponding operating system.

Hierarchical List of Anti-Virus Network

In the middle part of the window there is a hierarchical list of the anti-virus network. The list (catalog) represents the tree structure of the anti-virus network elements. The nodes in this structure are groups and workstations within these groups.

You can perform the following through the hierarchical list elements:

- Left-click the name of a group or station to display the control menu (at the left part of the window) of corresponding element and brief element information on a property pane (at the right part of the window).
- Left-click the icon of the group to open or to hide the contents of a group.
- Left-click the icon of the station to open the properties sheet of this station.

To select several elements of the hierarchical list, press and hold CTRL or SHIFT during selection.

The appearance of the icon depends on the type and status of this element (see table 2-1).

Table 2-1. Icons of elements in the hierarchical list

Icon	Description
	Groups. General icons
	Groups always shown in the hierarchical list.
	Groups are not displayed in the hierarchical list if: • for groups the **Setup group visibility** → **Hide if empty** option performed and currently groups do not contain stations, • for groups the **Setup group visibility** → **Hide** option performed and currently, in the **Settings of tree view** section, the **Show hidden groups** flag is cleared.
	Workstations. General icons
	Available workstations with installed anti-virus software.

Icon	Description
	The station is unavailable.
	Anti-virus software on the station is uninstalled.
	Station state during remote network installation of the **Agent**. Station is in this state from the moment of successful **Agent** installation on the station till the moment of its first connection to the **Server**.
	Additional icons
	Icon of personal settings is displayed over the general stations and groups icons for which personal settings are specified (or group includes stations with personal settings). To display the sign, select the **Settings of tree view** option on the toolbar and set the **Show personal settings icon** flag. E.g., if online workstation with installed anti-virus software has a personal settings, its icon looks as follows: .
	Icon of update error is displayed next to the general icons of stations on which errors during anti-virus software update occurred. To display the sign, select the **Settings of tree view** option on the toolbar and set the **Show update error icon** flag. E.g., if an error during anti-virus software update occurred on an online workstations, its icon looks as follows: .
	Icon of membership rules is displayed next to the general icon of groups for which rules of automatic stations placing are set. To display the sign, select the **Settings of tree view** option on the toolbar and set the **Show membership rules icon** flag. E.g., if a groups that is always shown in the hierarchical list has membership rules specified, its icon looks as follows: .

Management of the anti-virus network catalog elements is carried out via the toolbar of the hierarchical list.

Toolbar

The toolbar of the hierarchical list contains the following elements:

General. Manage the general parameters of the hierarchical list. Select the corresponding item in the drop-down list:

Edit. Opens settings of the station or group in the right pane of **Dr.Web Security Control Center**.

Remove selected objects. Remove an items from the hierarchical list. Select the items in the list and click **Remove selected objects**.

Remove membership rules. Remove rules for automatic including stations to groups.

Set this group as primary. Determine the selected group as primary for all workstations in it.

Set a primary group for stations. Assign a primary group for selected workstations. If a group is selected in the hierarchical list instead of workstations, the specified primary group will be assigned to all workstations from this group.

Merge stations. Join workstations under a single account in the hierarchical list. It can be used if a workstation had been registered under several accounts.

Remove personal settings. Remove individual settings of selected objects. Settings of the parent group will be used. All workstations inside a group will also have their settings removed.

Send message to stations. Send notifications to users of workstations.

Reset password. Allows to delete the user password for access to anti-virus components settings on selected stations. The option is available only for stations under Windows OS.

Reboot station. Launch reboot station process remotely.

Uninstall Dr.Web Agent. Remove the **Agents** and anti-virus software from the selected workstation(s) or group(s).

Install Dr.Web Agent. Open the Network scanner for **Agent** installation to the selected stations. This option is enabled only if new approved stations or stations with deinstalled **Agent** are selected.

Restore deleted stations. Allows to restore stations deleted earlier. This option is active only if stations from the **Deleted** subgroup of the **Status** group are selected.

Mail installation files. Send installation files for stations selected in the list to e-mail addresses, specified in this section parameters.

Add a station or a group. Add a new element of anti-virus network. Click the corresponding item in the drop-down menu:

Add station. Add a new station (see **Installation Manual**, p. Creation of a New User Account).

Add group. Add a new group.

Data Export. Save common data about workstations in the anti-virus network to a CSV, HTML or XML file. Select the file format in the drop-down menu.

Save in CSV format.

Save in HTML format.

Save in XML format.

Save in PDF format.

Export configuration.

Import configuration.

Propagate configuration.

Setup group visibility. Change the appearance of groups in the list. Select one of the following in the drop-down list (the icon of the group will change, see table 2-1):

Hide group - means that the group will not be displayed in the hierarchical list.

Hide if empty - means that the group will not be displayed if the group is empty (does not contain any workstations).

Show - means that the group will always be displayed in the hierarchical list.

Components management. Manage the components on the workstation. Select the necessary action in the drop-down menu:

Update all components. Update all installed components of the anti-virus, e.g., when the **Agent** has not been connected to the **Server** for a long time, etc. (see also p. Manual Updating of Dr.Web Enterprise Security Suite Components).

Update failed components. Force synchronization of the components that failed to update.

Interrupt running components. Prescribes to stop operating of all running anti-virus components at the station.

Scan. Scan stations in one of the modes, selected in the drop-down menu:

Dr.Web Scanner. Express scan. In this mode the following objects are scanned:

- main memory (RAM),
- boot sectors of all disks,
- autorun objects,

- root directory of the boot sector,
- root directory of the Windows OS installation disk,
- system directory of the Windows OS,
- `My documents` folder,
- temporary directory of the system,
- temporary directory of the user.

Dr.Web Scanner. Complete scan. In this mode all hard disks and removable disks (including the boot sectors) will be fully scanned.

Dr.Web Scanner. Custom scan. In this mode you will be able to choose files and folders to scan.

Unapproved stations. Manage newbies list - stations, which registration is not approved. This option is active only if stations of the **Newbies** subgroup of the **Status** group are selected. When the registration is approved or access to the **Server** is denied, stations will be automatically removed from the **Newbies** preinstalled group.

Approve selected stations and set a primary group. Prescribes to confirm access of the station to the **Server** and to set a primary group from the offered list.

Cancel action specified to execute on connect. Prescribes to cancel the action on unapproved stations which was specified earlier to execute at the moment when the station connects to the **Server**.

Reject selected stations. Prescribes to forbid access of the station to the **Server**.

Settings of tree view. Adjust the appearance of the list:

- for groups:
  - **All groups membership** – show a station in all groups it is a member of (only for groups under the white folder icon, see Table 2-1). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only in the top white folder.
  - **Show hidden groups** – show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing stations) will be hidden. It may be convenient to remove extra data, for example, when there are many empty groups.
- for stations:
  - **Show station ID** – enables/disables showing of stations unique identifiers in the hierarchical list.
  - **Show station names** – enables/disables showing of stations names in the hierarchical list, if such are given.
  - **Show station addresses** – enables/disables showing of stations IP-addresses in the hierarchical list.
  - **Show station servers** – enables/disables showing of names or addresses of **Dr.Web Servers** to which stations are connected.
  - **Show update error icon** – enables/disables marker on icon of workstations the last update of which is failed.
- for all elements:
  - **Show personal settings icon** – enables/disables marker on icon of workstations and groups which shows whether individual settings are present.
  - **Show descriptions** – enables/disables showing of groups and stations descriptions (the descriptions are set in the properties of an element).
  - **Show the number of stations** – enables/disables showing the number of stations for all groups of anti-virus network.
  - **Show membership rules icon** – enables/disables showing the mark on stations icons which are added to groups automatically according to the membership rules, also on groups icons in which stations are added automatically.

Property Pane

The property pane shows the properties and settings of workstations.

To display the property pane

1. Select the name of a station or a group in the hierarchical list.
2. A pane with properties of selected workstation or group opens in the right pane of **Dr.Web Security Control Center**. Detailed description of these settings is given in the Editing Groups and Station Properties.

2.3.3. Neighborhood

Select the **Neighborhood** item in the main menu of **Dr.Web Security Control Center**. The control menu in the left part of the window is used to select viewing information.

Administration

Administration section of the control menu contains the **Neighborhood** item, that serves to manage connections between **Servers** in a multi-server anti-virus network (for more details, see Peculiarities of a Network with Several Dr.Web Servers).

The hierarchical list represents all of **Dr.Web Server**, connected to this **Server**.

Setting of new interserver connections is described in Setting Connections between Several Dr.Web Servers.

Tables

The **Tables** section of the control menu contains information about the operation of the anti-virus network received from other **Servers** (see also Peculiarities of a Network with Several Dr.Web Servers).

To view the summary tables with data from other **Servers**, select the corresponding item in the **Tables** section.

2.3.4. Search Panel

The *search panel* locates at the top right part of **Dr.Web Security Control Center** and used to simplify searching for elements. The panel may find both groups and separate stations according to specified parameters.

To find a workstation or group of workstations:

1. Select the search criterion in the drop-down list of the search panel:
   - **Station -** to search stations by name,
   - **Group -** to search groups by name,
   - **ID -** to search stations and groups by unique identifiers,
   - **Description -** to search stations and groups by their description,
   - **IP address -** to search stations by their IP address.
   - **Hardware** - to search stations by the name of hardware installed on the station,
   - **Software** - to search stations by the name of software installed on the station.

2. Enter a parameter value to search. You can search values by specifying:
   - specific string for full match with search value,
   - a mask for search string: the * and ? symbols are allowed.
3. Press ENTER to start the search.
4. The search results contain a hierarchical list of elements according the search parameters.
   - If you searched for a workstation, occurrence of the workstation in groups will be displayed.
   - If no elements are found, the message **No results found** will be displayed in the empty hierarchical list.

2.3.5. Events

To notify administrator on events requiring attention, the section displayed under the **Events** icon on the main menu is provided.

The icon may take the following states:

– no new notifications on events in the network.

– new notifications on minor events.

– new notifications on major events requiring administrator intervention.

The following actions are available for the events list:

1. The icon click opens the drop-down list of anti-virus network events. At this, the icon automatically changes to .
2. The click on notification string on event opens the **Control Center** section that responsible for corresponding functions.
3. The stub of every notification in the events list is marked with a color corresponding to the severity of the events (same as the icon). When opening a section that responsible for the notification functions, the notifications is considered as read and the stub changes color into gray.

Table 2-2. The list of available notifications on events in anti-virus network

Event	Severity	Control Center section	Description
Install Dr.Web Security Control Center browser extension	minor	The page to download **Dr.Web Security Control Center** extension	Installation of **Dr.Web Security Control Center** extension required.
Unread news	minor	**Help → News**	Unread news of **Doctor Web** company are available.
New notifications	minor	**Administration → Web console notifications**	New administrator notifications which are received via the **Web console** method are available.
Critical notifications	major		
Server updates are available	major	**Administration → Dr.Web Server**	**Dr.Web Server** update is downloaded into repository and available for installation.
Server configuration has been changed. Server restart required.	major	**Administration → Dr.Web Server configuration**	Settings of the **Server** configuration file has been changed after **Server** start. To take new settings, the **Server** must be restarted.
Web server configuration has been changed. Server restart required.	major	**Administration → Web Server configuration**	Settings of the **Web server** configuration file has been changed after **Server** start. To take new settings, the **Server** must be restarted.

2.3.6. Preferences

To open the section of **Control Center** preferences, click **Preferences** in the main menu.

All settings of this section are valid only for the current administrator account.

The control menu located in the left pane of the window, consists of the following items:

- **My account**.
- **Interface**.
- **Subscription**.

My Account

Using this section, you can manage the current account of the administrator of the anti-virus network (see also p. Administrators and administrative groups).

Values of fields, marked with the * sign, must be obligatory specified.

You can edit the following settings, if necessary:

- **Login** - administrator account login to access **Dr.Web Security Control Center**.
- **First name**, **Middle name** and **Last name** of the administrator.
- **Interface language** used by the administrator.
- **Date format**, which is used by this administrator during editing settings that contain dates. The following formats are available:
  - European: `DD-MM-YYYY HH:MM:SS`
  - American: `MM/DD/YYYY HH:MM:SS`
- Account **Description**.
- To change the password, click **New password** at the toolbar.

The following parameters are read only:

- Dates of creation and last modification of the account.
- **Status**. Displays the network address of the last connection under this account.

Rights of the administrator

Description of administrative rights and its editing see in the Editing Administrators section.

Click **Save** after you have changed all necessary parameters.

Interface

Tree settings

Parameters of this section let you adjust the appearance of the list and they are similar to the settings, located in the option of the toolbar of the **Anti-virus network** item of the main menu.

- for groups:

- **All groups membership** – show a station in all groups it is a member of (only for groups under the white folder icon, see Table 2-2). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only in the top white folder.
- **Show hidden groups** – show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing stations) will be hidden. It may be convenient to remove extra data, for example, when there are many empty groups.

◆ for stations:

- **Show station ID** – enables/disables showing of stations unique identifiers in the hierarchical list.
- **Show station names** – enables/disables showing of stations names in the hierarchical list, if such are given.
- **Show station addresses** – enables/disables showing of stations IP-addresses in the hierarchical list.
- **Show station servers** – enables/disables showing of names or addresses of **Dr.Web Servers** to which stations are connected.
- **Show update error icon** – enables/disables marker on icon of workstations the last update of which is failed.

◆ for all e llements:

- **Show personal settings icon** – enables/disables marker on icon of workstations and groups which shows whether individual settings are present.
- **Show descriptions** – enables/disables showing of groups and stations descriptions (the descriptions are set in the properties of an element).
- **Show the number of stations** – enables/disables showing the number of stations for all groups of anti-virus network.
- **Show membership rules icon** – enables/disables showing the mark on stations icons which are added to groups automatically according to the membership rules, also on groups icons in which stations are added automatically.

Network scanner

The **Network scanner** requires **Dr.Web Security Control Center Extension**.

The settings of this section let you configure the default parameters of Network Scanner.

To launch the **Network scanner**, select **Administration** item in the main menu. In the control menu, select **Network scanner**.

Specify the following parameters of **Network scanner**:

1. In the **Networks** field specify networks in the following format:
   ◆ with a hyphen (for example, `10.4.0.1-10.4.0.10`)
   ◆ separated by a comma with a whitespace
   (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`)
   ◆ with a network prefix (for example, `10.4.0.0/24`).
2. Change **Port** and **Timeout** parameters, if necessary.
3. Click **Save** to save these parameters as default. After that, when you use the Network scanner, this parameters will be set automatically.

Time Interval

In this section, you can specify settings of time interval to display statistics data (see Viewing Workstation Statistics section):

- In the **Default interval for viewing statistics data** drop-down list, specify the time interval, which is set as default for all sections of statistics data.

  When you open the page for the first time, statistics will be displayed for this time interval. You can change the time interval at statistics pages directly, if necessary.

- Set the **Save last interval for statistics data** flag, to save the interval, specified last time at statistics sections.

  If the flag is set, when you open the page for the first time, statistics will be displayed for the last period, specified at the Web browser.

  If the flag is cleared, when you open the page for the first time, statistics will be displayed for the period, specified in the **Default interval for viewing statistics data** drop-down list.

Authorization

Set the **Automatic authorization** flag to allow automatic authorization for all **Control Centers** with the same administrator's login and password in the current browser.

After setting this flag, login and password specified by administrator at next logon in the **Control Center**, will be saved via the **Dr.Web Security Control Center Extension**.

Automatic authorization option requires **Dr.Web Security Control Center Extension**.

Further, for any **Control Center** in this web browser, authorization will be proceeded automatically, if the user with these login and password is registered at the **Server**. If the login and password do not much (e.g., such user is not registered or the user with this name has the different password), the standard **Dr.Web Security Control Center** authorization window will be given.

After clicking **Logout** in the main menu of the **Control Center**, information about administrator's login and password is deleted.

At next logon in the **Control Center**, it is necessary to repeat standard authorization procedure with specifying login and password. If automatic authorization is enabled, specified login and password are saved for the current web browser and authorization in **Control Center** become automatic (without login and password confirmation) till next **Logout** clicking.

In the **Session timeout** drop down list, select time period after which the user session of **Control Center** in a web browser is automatically terminated.

PDF Export

In this section you can specify text settings for statistic data export to the PDF format:

- In the **Reports font** drop down list, select the font, which is used at reports export to PDF format.
- In the **Reports font size** field, specify the font size of general text of statistic tables, which is used at reports export to PDF format.

Reports

In this section you can specify view settings for statistic data in the Reports section of the **Control Center**:

- In the **Number of lines per page** field, specify the maximal number of lines on one report page for paginal view of statistic.
- Set the **Show charts** flag to show charts on statistic reports pages. If the flag is cleared, charts viewing is disabled.

Subscription

In this section you can setup the subscription on **Doctor Web** company news.

Set the **Automatic subscription to new sections** flag to add new sections in the **News** page of **Control Center** automatically.

2.3.7. Help

To open the **Help** section of **Dr.Web Security Control Center**, click **Help** in the mail menu.

The control menu in the left part of the window contains the following elements:

1. **General**
   - **Forum** – opens official forums of **Doctor Web** company.
   - **News** – open the news page of **Doctor Web** company.
   - **Contact technical support service** – opens the web page of **Doctor Web** technical support.
   - **Send a suspect file** – opens a web form for sending a virus to **Dr.Web Virus Laboratory**.
   - **Report false alarm in Office Control** – opens a web form for sending a message about false alarm or detection failure in **Office Control** module.
2. **Administrative Documentation**
   - **Installation manual** – opens documentation on **Dr.Web Enterprise Security Suite** installation in HTML format.
   - **Administrator manual** – opens administrator documentation in HTML format.
   - **Appendices** – opens appendices of administrator manual in HTML format.
   - **Web API Manual** – opens administrator documentation on XML Web API (see also the **Appendices** document, p. Appendix L. Integration of Web API and Dr.Web Enterprise Security Suite) in HTML format.
   - **Release notes** – opens release notes for **Dr.Web Enterprise Security Suite** of installed version.
3. **User Documentation** – opens user documentation for corresponding operating system in HTML format from the list.

2.4. Dr.Web Security Control Center Components

2.4.1. Network Scanner

Dr.Web Server contains the **Network Scanner** component.

It is not recommended to launch the **Network Scanner** under Windows 2000 and earlier operating systems due to possible insufficiencies of network review.

The functioning of the **Network Scanner** is guarantied under UNIX system-based operating systems and Windows XP or later.

The **Network scanner** requires **Dr.Web Security Control Center Extension**.

For correct functioning of the **Network Scanner** under Windows Internet Explorer browser, you must add **Dr.Web Security Control Center** address into which the **Network Scanner** is launched, to the list of trusted sites in the web browser settings: **Tools** → **Internet Options** → **Security** → **Trusted Sites**.

Network Scanner provides the following functions:

- Scan (browse) the network for workstations.
- Detect **Dr.Web Agents** on stations.
- Install **Dr.Web Agent** on the detected stations as instructed by the administrator. **Dr.Web Agent** installation is described in detail in the **Installation Manual**, p. Installing Dr.Web Agent Software via Dr.Web Security Control Center.

To scan (browse) the network, perform the following actions:

1. Open the **Network Scanner** window: select the **Administration** item in the main menu of **Dr.Web Security Control Center** and in the opened window, select the **Network Scanner** item in the control menu. The **Network Scanner** window will be opened.
2. Set the **Search by IP addresses**, flag to search for stations in the network by specified IP addresses. In the **Networks** field specify networks in the following format:
   - with a hyphen (for example, `10.4.0.1-10.4.0.10`)
   - separated by a comma with a whitespace (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`)
   - with a network prefix (for example, `10.4.0.0/24`).
3. For Windows OS: set the **Search in Active Directory** flag to search for stations in the Active Directory domain. At this, specify the following parameters:
   - **Domains** - domains list in which stations are searched. Use comma to divide several domains.
   - **Active Directory controller** - Active Directory controller, e.g., dc.example.com.

To be able to search stations in the Active Directory domain via the **Network Scanner**, the web browser in which the **Control Center** is opened, must be launched in the name of the domain user with permissions to search objects in the Active Directory domain.

4. For UNIX system-based OS: set the **Search by LDAP** flag to search for stations by LDAP. At this, specify the following parameters:
   - **Domains** - domains list in which stations are searched. Use comma to divide several domains.
   - **LDAP server** - LDAP server, e.g., ldap://ldap.example.com.
   - **Login** - LDAP user login.
   - **Password** - LDAP user password.

5. In the **Port** field, specify the port to connect via the UDP protocol to the **Agents** during search.
6. If necessary, in the **Timeout** field, change the value of timeout in seconds, which defines time limit for receiving an answer from inquired stations.
7. If necessary, set the **Quick scan** flag for express scanning.
8. Set the **Show station names** flag to display either IP address and DNS name of found network stations.

   If a station is not registered at DNS server, only its IP address displays.

9. Set the **Correlate with stations list from database** flag to enable synchronization of **Network Scanner** search results with the stations list stored in the **Server** DB. If the flag is set, the list of found network stations contains stations from the **Server** DB list that are not found by the **Network Scanner** during current search, e.g. if a firewall installed at stations blocks the transfer of packets needed to establish a TCP connection.

   During synchronization of **Network Scanner** search results with **Server** DB data, the **Server** DB data has priority, i.e. if station statuses from search results and from DB are differ, the status from DB is set.

10. Click the **Scan** button to launch network scanning.
11. The catalog (hierarchical list) of computers demonstrating where **Dr.Web Enterprise Security Suite** anti-virus software is installed will be loaded into this window.

    Unfold the catalog elements corresponding to workgroups (domains). All elements of the catalog corresponding to workgroups and individual stations are marked with different icons the meaning of which is given below.

Table 2-3. Icons of the Network scanner

Icon	Meaning
Workgroups	
	The work groups containing inter alia computers on which **Dr.Web Enterprise Security Suite** anti-virus software can be installed.
	Other groups containing protected or unavailable by network computers.
Workstations	
	The detected station is registered in the DB and active (i.e. the workstation with installed anti-virus software).
	The detected station is registered in the DB as deleted (i.e. the workstation is listed in the table of deleted stations).
	The detected station is not registered in the DB (i.e. there is no anti-virus software on the station).
	The detected station is not registered in the DB (the station is connected to another **Server**).
	The detected station is registered in the DB, bus it is not active and the port is closed.

You can also unfold catalog items corresponding to computers with the or icon, and check which program components are installed there.

Click the icon of component at the station, connected to this **Server**, to open component settings window.

Interaction with Dr.Web Agent

The **Network Scanner** tool has been included in **Dr.Web Enterprise Security Suite** starting from version **4.44**.

Network Scanner can detect **Agents** of version **4.44** and older but cannot interact with **Agents 4.33**.

Dr.Web Agents 4.44 and older installed on protected stations process respective calls of **Network Scanner** received at a certain port. By default port `udp/2193` is using, but also port `udp/2372` is supported for compatibility with older versions. Correspondingly, it is the default port offered by the **Scanner** to call at. **Network Scanner** decides whether there is an **Agent** on the workstation based on the assumption of the possibility to exchange information with the station (request-response) through the specified port.

If the station is forbidden (for example, by a firewall) to accept packages at `udp/2193`, the **Agent** will not be detected and consequently **Network Scanner** considers that there is no **Agent** installed on the station.

Quick Scan

If the **Quick scan** option is enabled, the following actions will be performed:

1. Ping requests are sent to network computers.
2. The parallel poll for **Agents** detection is performed only for computers which has answered to ping requests.
3. **Agents** detection procedure is implemented according to general rules.

Ping requests can be blocked because of network policies (e.g. by firewall settings).

For example:

If in Windows Vista and later OS network settings the **Public location** options is set, OS will block all ping requests.

During regular scanning, ping requests are not sent and all stations in the network are sequentially scanned to detect **Agents**. This method can be used as an addition to quick scan, if there are stations in the network, whereon ping requests are blocked.

Quick scan is parallel, regular scan is sequential.

The **Network scanner** operating speed is different for these cases. Maximal scanning time is calculated in the following way:

- for regular scan: <*N*> * <*timeout*>,
- for quick scan: <*N*>/40 + 2*<*timeout*>,

where: <*N*> - stations quantity, <*timeout*> - value, specified in the **Timeout** field.

2.4.2. License Manager

Licensing Features

1. **Dr.Web Server** is not licensed. **Server** can be installed without license key. The key can be added later either locally or received via the interserver communication.

   Server UUID which was stored in a **Server** license key in the previous versions of **Dr.Web Enterprise Security Suite**, starting from the **10.0** version, is stored in the **Server** configuration file.

   - During the new **Server** installation, the new UUID is generated.
   - During the **Server** update from the earlier versions, UUID is automatically taken from the **Server** key of previous version (the `enterprise.key` file from the `etc` folder of the previous **Server** installation) and is written to the configuration file of the installing **Server**.

   When updating the **Servers** cluster, the **Server** which is responsible for DB updating, gets a license key, for other **Servers** it is necessary to add license keys manually.

2. License keys are actual for protected stations only. You can assign a key file either for separate stations or for stations groups: in this case, a license key is valid for all stations which inherit it from this group. To assign the key file simultaneously for all stations of anti-virus network, for which personal settings of license key are not specified, assign the license key for the **Everyone** group.
3. Via the interserver communication, optional number of licenses from keys at this **Server** can be donated to a neighbor **Server** for a specified time slot.
4. Each license key can be assigned for several licensing objects (groups and stations) simultaneously. For one licensing object can be assigned several license keys simultaneously.
5. When you assigning several keys to the object, please consider the following features:
   a) If lists of allowed anti-virus components in several keys of one object differ, when the list of allowed components for this station is defined by intersection of keys components sets. E.g., if for stations group a key with **Anti-spam** support and a key without **Anti-spam** support are assigned, when the **Anti-spam** cannot be installed on the stations.
   b) Settings for object licensing are calculated according of all keys assigned to this object. If keys expiration dates are differ, after nearest expiration date is out, you need to replace or remove expired key manually. If expired key limits an anti-virus components installation, it is necessary to adjust licensing object settings in the Installing Components section.
   c) The number of licenses of the object is calculated as a sum of licenses from all the keys which are assigned to this object. Also consider the opportunity to donate licenses via the interserver communication to a neighbor **Server** (see p. 3). In this case, you should subtract the licenses donated to a neighbor **Server** from the total number of licenses.

License key file is set during the installation of **Dr.Web Server** (see **Installation Manual**, p. Installing Dr.Web Server). Further you can get new key files, e.g. with longer license validity time or other set of anti-virus components for protected stations.

The key file has a write-protected format using a digital signature. Editing the key file makes it invalid. To avoid this, do not modify the key file and/or save it when closing the text editor.

License Manager Interface

Dr.Web Security Control Center contains the **License Manager** component. This component is used to manage licensing of anti-virus network objects.

To open the **License manager**, select **Administration** item in the main menu of **Dr.Web Security Control Center**. In the opened window select the **License manager** item in the control menu.

Keys Hierarchical List

The main pane of the **License manager** contains keys tree - the hierarchical list nodes of which are license keys of stations and groups for which license keys are assigned.

Toolbar contains the following control elements:

Option	Description	Dependence on objects in the keys tree
Add key	Add a new license key record.	Option is always available. Functional features depend on whether the object is selected in the key tree or not (see Add a new license key).
Remove selected objects	Remove the connection between the key and the licensing object.	Option is available if a licensing object (station or group) or a license key is selected in the tree.
Propagate the key to groups and stations	Replace of add selected key to a licensing object.	Option is available if a license key is selected in the tree.
Export key	Save the local copy of the license key file.	
Propagate the key to neighbor Servers	Donate licenses from the selected key to neighbor **Servers**.	

Settings of tree view allows to change hierarchical tree view:

- The **Show the number of licenses** flag enabled/disables displaying in the keys tree the total number of licenses provided by key files.
- To change the tree structure, use the following options:
  - The **Keys** option prescribes to display all license keys of anti-virus network as a root nodes of the hierarchical tree. At this, all groups and stations for which these keys are assigned, are presented as a child elements of license keys. This tree view is a general view and allows to manage licensing objects ans license keys.
  - The **Groups** option prescribes to display those groups to which the keys are personally assigned as a root nodes of the hierarchical tree. At this, stations included in this groups and license keys that are assigned to these groups are presented as a child element of groups. This tree view is for convenience visualization of information on licensing and do not allow to manage objects of the tree.

Licenses Handling

Via the License Manager you can perform the following actions under license keys:

1. View Information About a License.
2. Add a New License Key.
3. Update the License Key.
4. Replace the License Key.
5. Extend the List of Object License Keys.
6. Remove the License Key and the Object from the Licensing List.
7. Donate a License to a neighbor Server.

8. Edit Licenses Donated to a Neighbor Server.

View Information About a License

To view the summaries about the license key, in the main pane of the **License manager**, select the key record to view the detail information (click the key record name). In the opened pane you can view the following information:

- the owner of the license,
- the dealer, who sold the license,
- identification and serial numbers of the license,
- license expiration date,
- Inclusion of the **Anti-spam** component,
- number of stations to license by this key file,
- MD5 hash of the license key,
- the list of anti-virus components which are allowed to use by this license.

Add a New License Key

To add a new license key:

1. In the main pane of the **License Manager**, click **Add key** on the toolbar.
2. On the opened panel, click and select the license key file.
3. Click **Save**.
4. The license key will be added to the keys tree but not assigned neither to one of the objects. In this case, to specify licensing objects, perform the Change the License Key or Extend the List of Object License Keys procedures described below.

Update the License Key

In updating a license key, the new license key is assigned for the same licensing objects, for which the updated one was assigned.

Use the updating key procedure to replace expired key or to replace with a key with other set of installing components. The keys tree structure remains.

To update a license key:

1. In the main pane of the **License Manager** in the keys tree, select the key you want to update.
2. On the opened key properties panel, click and select the license key file.
3. Click **Save**. A window with installed components settings described in Settings for License Key Changing, opens.
4. Click **Save** to update the license key.

Replace the License Key

In changing a license key, all current license keys are deleted for the licensing object and a new key is added.

To replace the current license key:

1. In the main pane of the **License Manager** in the keys tree, select the key you want to assign to the licensing object.

2. Click **Propagate the key to groups and stations** on the toolbar. A window with hierarchical list of stations and groups of anti-virus network opens.
3. Select licensing object from the list. To select several stations or groups, use CTRL and SHIFT.
4. Click **Replace key**. A window with installed components settings described in Settings for License Key Changing, opens.
5. Click **Save** to replace the license key.

Extend the List of Object License Keys

In adding a license key, the licensing object saves all current keys, and to the keys list a new license key is added.

To add the license key to the object license keys list:

1. In the main pane of the **License Manager** in the keys tree, select the key you want to add to the objects keys list.
2. Click **Propagate the key to groups and stations** on the toolbar. A window with hierarchical list of stations and groups of anti-virus network opens.
3. Select licensing object from the list. To select several stations or groups, use CTRL and SHIFT.
4. Click **Add key**. A window with installed components settings described in Settings for Adding a License Key to the Keys List, opens.
5. Click **Save** to add the license key.

Remove the License Key and the Object from the Licensing List

> You cannot remove the last license key record of the **Everyone** group.

To remove the license key or the object from the licensing list:

1. In the main pane of the **License Manager** in the keys tree, select the key you want to remove, or the object (station or group), to which this key is assigned, and click **Remove selected objects** on the toolbar. At this:
   - If the licensing object was selected, this object will be removed from the list of objects on which its key is effects. An object for which a personal license key is removed, inherits a license key.
   - If the license key was selected, this key record is removed from the anti-virus network. All objects to which this license key was assigned, inherit a license key.
2. A window with installed components settings described in Settings for License Key Changing, opens.
3. Click **Save** to remove selected object and to switch to the inherited key.

Donate a License to a neighbor Server

At donating a part of vacant licenses to a neighbor **Server** from the license key of this **Server**, donated number of licenses will not be available for use on this **Server** till the end of propagation time of these licenses.

To donate licenses to a neighbor Server:

1. In the main pane of the **License Manager** in the keys tree, select the key a vacant licenses from which you want to donate to neighbor **Server**.
2. Click **Propagate the key to neighbor Servers** on the toolbar. A window with hierarchical tree of neighbor **Server** opens.

3. Select from the list those **Servers** to which you want propagate licenses.
4. Specify the following parameters next to the each **Server**:
   - **Number of licenses** - number of vacant licenses, you want to donate from this key to a neighbor **Server**.
   - **License expiration date** - validity period of licenses donation. After specified time period, all licenses will be recall from the neighbor **Server** and got back to the list of vacant licenses in this license key.
5. Click on of the buttons:
   - **Add key** - to add licenses to the list of presence licenses of neighbor **Servers**. A window with installed components settings described in Settings for Adding a License Key to the Keys List, opens.
   - **Replace key** - to remove current licenses of neighbor **Servers** and set only propagated licenses. A window with installed components settings described in Settings for License Key Changing, opens.
6. Click **Save** to propagate licenses to neighbor **Servers**.

Edit Licenses Donated to a Neighbor Server

To edit licenses propagated to neighbor Server:

1. In the main pane of the **License Manager** in the keys tree, select the neighbor **Server**, on which licenses were propagated.
2. On the opened properties panel, edit the following parameters:
   - **Number of licenses** - number of vacant licenses, which were donated from the key of this **Server** to the neighbor **Server**.
   - **License expiration date** - validity period of licenses donation. After specified time period, all licenses will be recall from the neighbor **Server** and got back to the list of vacant licenses in this license key.
3. Click **Save** to update information on propagated licenses.

Changing the List of Installed Components

Settings for License Key Changing

In this section you can find description of installing components setup for the following procedures:

- Update the License Key.
- Replace the License Key.
- Remove the License Key.
- Donate a License to a neighbor **Server** with replacing a key.

When performing these procedures, to setup installing components, do the following:

1. In the window with installed components settings, the following objects are listed:
   - Stations and groups with their list of installing components.
   - In the **Current key** column, you can find the list of object keys and settings of installing components that are currently actual for the object.
   - In the **Assigned key** column, you can find the key and settings of installing components that are specified in the key which you want to assign to the selected objects.
2. If necessary, set the **Show only different** flag to show in the list only those components settings of which in the current and assigned keys are differ.
3. To configure the list on installed components:

a) In the **Assigned key** column, you can configure the result list of installing components.

- Installing components settings in the **Assigned key** column, are calculated on the basis of that if use the component in the current settings and in the new key is allowed (+) or not allowed (-), as follows:

Current settings	Assigned key settings	Result settings
+	+	+
–	+	+
+	–	–
–	–	–

- You can change installing components settings (downgrade rights to install) only if settings calculated in the **Assigned key**, allow to use this component.

b) Set the flags for those objects (stations and groups) for which settings inheritance will be terminated and installing components settings from the **Assigned key** column are set as a personal. For other objects (for which flags are not set), initial settings from the **Assigned key** column are inherited.

Settings for Adding a License Key to the Keys List

In this section you can find description of installing components setup for the following procedures:

- Extend the List of Object License Keys.
- Donate a License to a neighbor **Server** with adding a key.

When performing these procedures, to setup installing components, do the following:

1. In the window with installed components settings, the following objects are listed:
   - Stations and groups with their list of installing components.
   - In the **Current key** column, you can find the list of object keys and settings of installing components that are currently actual for the object.
   - In the **Assigned key** column, you can find the key and settings of installing components that are specified in the key which you want to add to the selected objects.
2. If necessary, set the **Show only different** flag to show in the list only those components settings of which in the current and assigned keys are differ. Note that in the **Assigned key** section not the assigned key settings are listed, but the result settings of installing components.
3. To configure the list on installed components:

   a) In the **Assigned key** column, you can configure the result list of installing components.

   - Installing components settings in the **Assigned key** column, are calculated on the basis of that if use the component in the current settings and in the new key is allowed (+) or not allowed (-), as follows:

Current settings	Assigned key settings	Result settings
+	+	+
–	+	–
+	–	–
–	–	–

   - You can change installing components settings (downgrade rights to install) only if settings calculated in the **Assigned key**, allow to use this component.

b) Set the flags for those objects (stations and groups) for which settings inheritance will be terminated and installing components settings from the **Assigned key** column are set as a personal. For other objects (for which flags are not set), initial settings from the **Assigned key** column are inherited.

2.5. The Interaction Scheme of an Anti-Virus Network Components

The Figure 2-2 describes a general scheme of an anti-virus network built with **Dr.Web Enterprise Security Suite**.

The scheme illustrates an anti-virus network built with only one **Server**. In large companies it is worthwhile installing several **Dr.Web Servers** to distribute the load between them.

In this example the anti-virus network is implemented within a local network, but for the installation and operation of **Dr.Web Enterprise Security Suite** and anti-virus packages the computers need not be connected within any local network, Internet connection is enough.

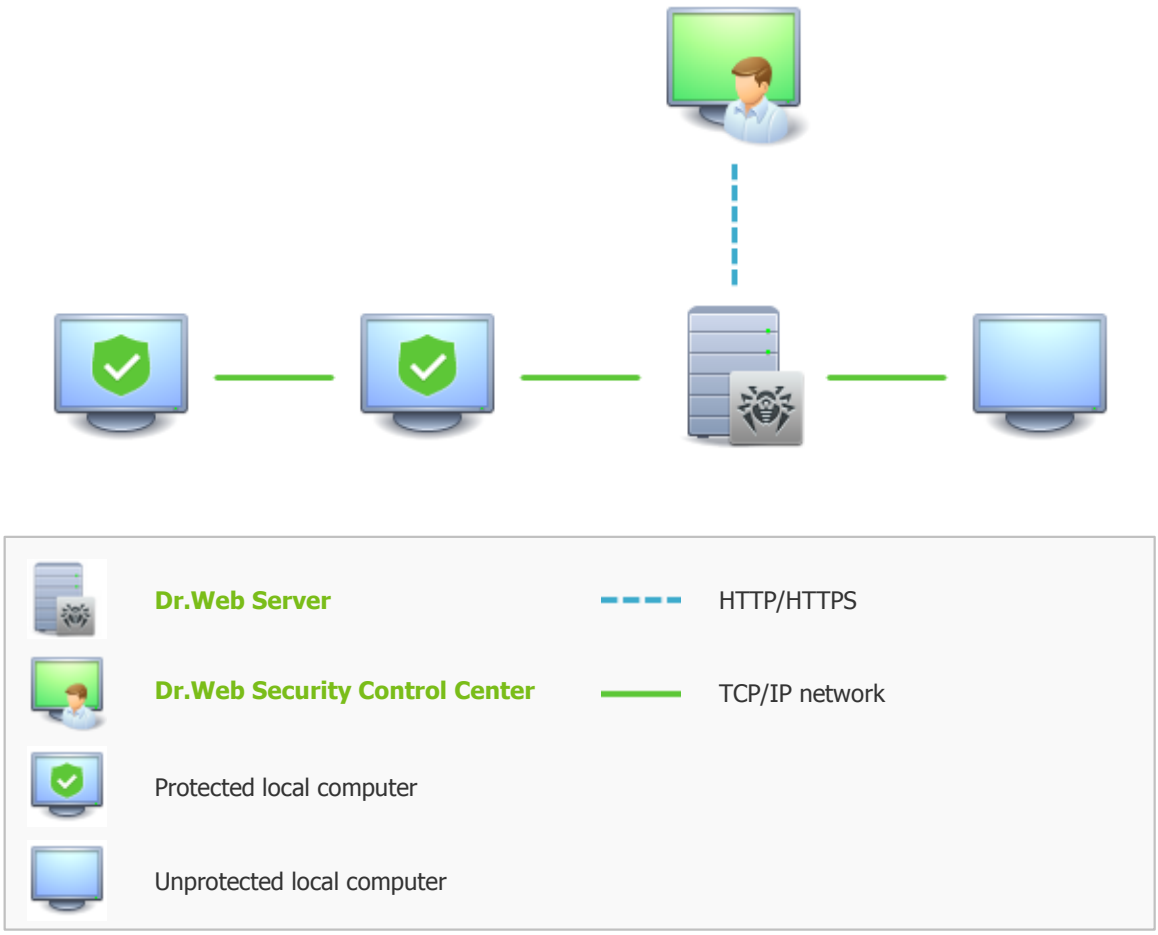


Figure 2-2. The physical structure of the anti-virus network

When Dr.Web Server is launched, the following sequence of commands is performed:

1. **Dr.Web Server** files are loaded from the `bin` catalog.
2. The **Server Task Scheduler** is loaded.

3. The content of the centralized installation catalog and update catalog is loaded, notification system is initialized.
4. **Server** database integrity is checked.
5. **Server Task Scheduler** tasks are performed.
6. The **Server** is waiting for information from **Dr.Web Agents** and commands from **Dr.Web Security Control Center**.

The whole stream of instructions, data and statistics in the anti-virus network always goes through **Dr.Web Server**. **Dr.Web Security Control Center** exchange information only with **Servers**. Based on **Dr.Web Security Control Center** commands, **Servers** transfer instructions to **Dr.Web Agents** and change the configuration of workstations.

Thus, the logical structure of the fragment of the anti-virus network looks as in the Figure 2-3.

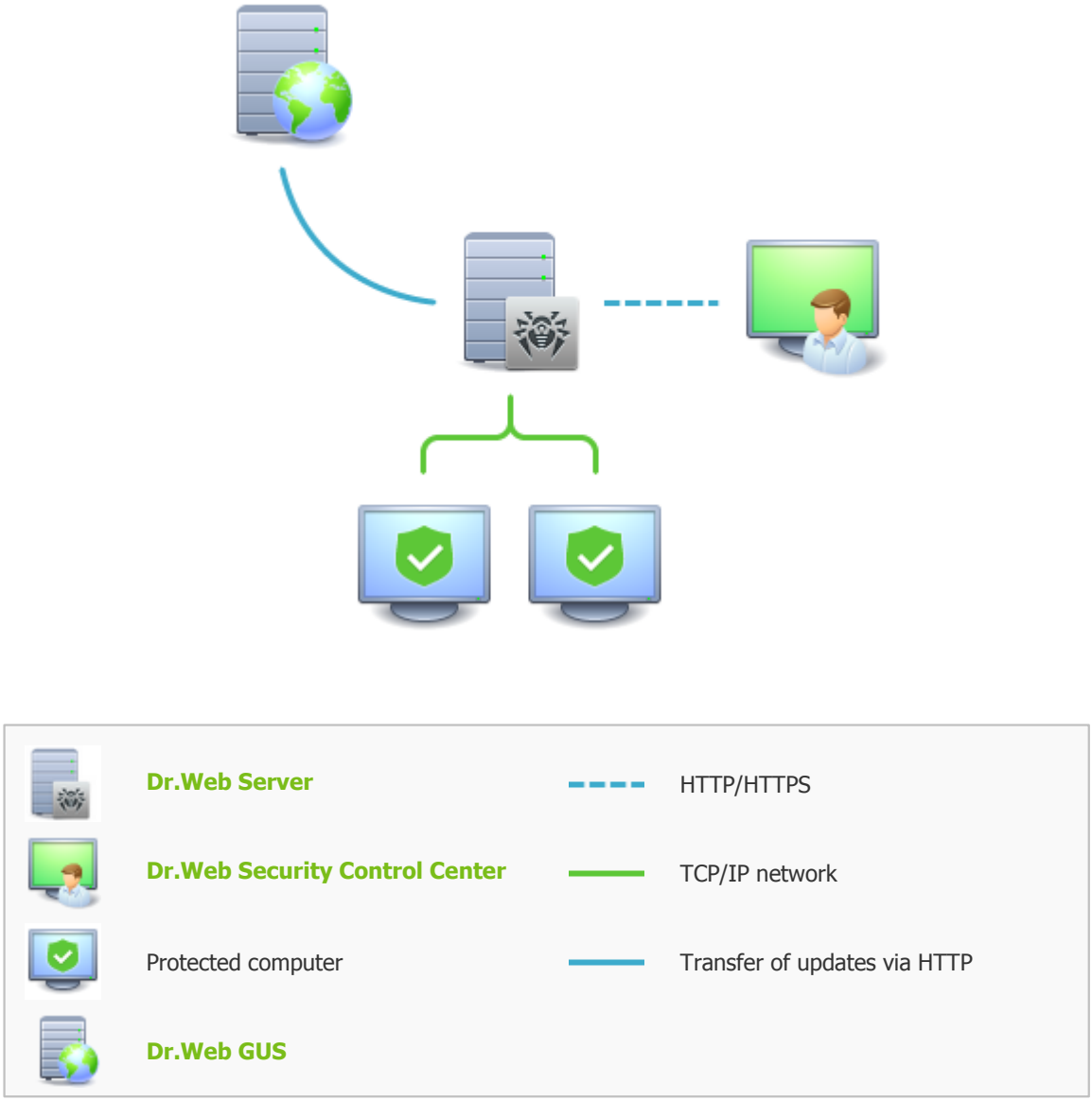


Figure 2-3. The logical structure of the anti-virus network

Between the **Server** and workstations (a thin continuous line in the Figure 2-3) transferring the following information:

- **Agents** requests for the centralized schedule and the centralized schedule of workstations,

- settings of the **Agent** and the anti-virus package,
- requests for scheduled tasks to be performed (scanning, updating of virus databases, etc.),
- files of anti-virus packages – when the **Agent** receives a task to install them,
- software and virus databases updates – when an updating task is performed,
- **Agent** messages on the configuration of the workstation,
- statistics (to be added to the centralized log) on the operation of **Agents** and anti-virus packages,
- messages on virus events and other events which should be logged.

The volume of traffic between the workstations and the **Server** can be quite sizeable subject to the settings and the number of the workstations. Therefore **Dr.Web Enterprise Security Suite** provides for the possibility to compress traffic. See the description of this optional mode in p. Traffic Encryption and Compression below.

Traffic between **Dr.Web Server** and **Dr.Web Agent** can be encrypted. This allows to avoid disclosure of data transferred via the described channel as well as to avoid substitution of software downloaded onto workstations. By default traffic encryption is enabled (for more, please read p. Traffic Encryption and Compression).

From the update web server to **Dr.Web Server** (a thick continuous line in the Figure 2-3) files necessary for replication of centralized catalogs of installation and updates as well as overhead information on this process are sent via HTTP. The integrity of the information (**Dr.Web Enterprise Security Suite** files and anti-virus packages) is provided through the checksums: a file corrupted at sending or replaced will not be received by the **Server**.

Between the **Server** and **Dr.Web Security Control Center** (a dashed line in Figure 2-3) data about the configuration of the **Server** (including information about the network layout) and workstations settings are passed. This information is visualized on **Dr.Web Security Control Center**, and in case a user (an anti-virus network administrator) changes any settings, the information about the changes is transferred to the **Server**.

Connection between **Dr.Web Security Control Center** and a certain **Server** is established only after an anti-virus network administrator is authenticated by his login name and password on the given **Server**.

Chapter 3: Getting Started. General Information

3.1. Establishing a Simple Anti-Virus Network

Before using the anti-virus software it is recommended to change the settings of the backup folder for the **Server** critical data (see p. Setting Dr.Web Server Schedule). It is advisable to keep the backup folder on another local disk in order to reduce the risk of losing **Server** software files and backup copies at the same time.

Connecting via Dr.Web Security Control Center

The **Server** is started automatically once the installation of the **Server** is complete (see also Dr.Web Server).

To set up the **Server** and configure the anti-virus software, **Dr.Web Security Control Center** should be run on the computer of the administrator and a connection to the **Server** should be established.

From any computer with network access to the **Server**, **Dr.Web Security Control Center** is available at the following address:

`http://`*<Server_Address>*`:9080`

or

`https://`*<Server_Address>*`:9081`

where *<Server_Address>* is the IP address or domain name for the computer on which **Dr.Web Server** is installed.

In the authorization dialog window specify the user name and password of the administrator (by default, administrator name is **admin** and the password is the same, as was specified during **Server** installation, see **Installation Manual**, p. Installing Dr.Web Server).

If registration at the **Server** is successful, the main **Dr.Web Security Control Center** window will be opened. In this window information on the anti-virus network managed from this **Server** can be viewed (for details, see p. Dr.Web Security Control Center).

Anti-virus Network Managing

Now you can administer the **Server** and the anti-virus network:

- create anti-virus stations (see **Installation Manual**, p. Installing Dr.Web Agent),
- approve stations,
- edit, configure and remove anti-virus stations (see Chapter 6: Administration of Workstations),
- configure and edit connections with neighbor **Dr.Web Servers** (see Peculiarities of a Network with Several Dr.Web Servers),
- view logs of current and neighbor **Dr.Web Servers** and other data.

Main controls are placed on the main menu, the control menu and the toolbar (see Dr.Web Security Control Center).

Connecting of Dr.Web Agent

After the **Agent** has been installed on a workstation via the installation package (see **Installation Manual**, p. Installation Files), it will try to establish a connection with the **Server**.

With default **Server** settings new workstations should be approved by an administrator to be registered at the **Server** (for more about the policy of connecting new workstations, please refer to p. New Stations Approval Policy). In this mode new workstations are not connected automatically, but placed by the **Server** into the newbies group (see p. System and User Groups).

Anti-Virus Software Installation

Installation of other software components (of **Agent** and anti-virus package) is proceeded without administrator intervention.

Anti-virus components, specified at the primary group settings, are installed on the station (for more details see Installing Components of the Anti-Virus Package).

To finish the installation of some components for anti-virus workstations you will need to restart the computer. In this case, there will appear a red exclamation mark over **Dr.Web Agent** icon in the **Taskbar** (see also Dr.Web Agent).

3.2. Setting the Network Connections

General Information

The following clients are connected to **Dr.Web Server**:

- **Dr.Web Agents**,
- **Network Installers** of **Dr.Web Agents**,
- other **Dr.Web Servers**.

Connection is always initiated by a client.

The following schemas for connection to the **Server** are available:

1. Using Direct connections.

   This approach has a lot of advantages, but it is not preferable in some situations (also, there are some situations, that are not compatible with this approach).

2. Using Server Detection Service.

   Clients use this **Service** by default (if the other is not set obviously).

   You can use this approach, if the resetting of all system is needed, in particular, if you need to move the **Server** to another computer or change the IP-address of a computer with the **Server**.

3. Using the SRV protocol.

   This approach allows to search the **Server** by name of a computer or **Server** service via the SRV records at DNS server.

If you configure the anti-virus network for using the direct connections, the **Server Detection Service** can be disabled. To do this, at the transport settings (**Administration** → **Dr.Web Server configuration** → **Transport** tab) leave the **Cluster address** field empty.

Firewall Setup

For anti-virus network components communication, all ports and interfaces, which are used by this components, must be opened on all computers in the anti-virus network.

During **Server** installation, the installer allows to add an exceptions to OS firewall settings. To do this, set the **Add Server ports and interfaces to firewall exceptions** flag.

If a non-built-in Windows firewall is in use, the network administrator should set it up manually.

3.2.1. Direct Connections

Dr.Web Server Setup

In the **Server** settings the address must be set (see the **Appendices** document, p. Appendix E. The Specification of Network Addresses) to listen for accepting incoming TCP-connections.

You can specify this parameter in the following **Servers** settings: **Administration** → **Dr.Web Server configuration** → **Transport** tab → **Address** field.

By default, the following parameters are set to "listen" by the **Server**:

- **Address**: empty value - use "all network interfaces" for this computer, on which the **Server** is installed.
- **Port**: `2193` - use the `2193` port, registered for **Dr.Web Enterprise Security Suite** in IANA.

Note: in **Servers 4.XX** the `2371` port was used. In the **10.0** version this port is no longer supported.

For the proper functioning of all **Dr.Web Enterprise Security Suite** anti-virus network, it is enough for the **Server** to listen at least one TCP-port, which is known by all clients.

Dr.Web Agent Setup

During the **Agent** installation, the **Server** address (IP-address or hostname of the computer, on which the **Server** is launched) can be directly set in installation parameters:

`drwinst` <*Server_Address*>

For the **Agent** installation it is recommended to use the **Server** name, registered in DNS service. This will simplify the setting of the anti-virus network in case of moving **Dr.Web Server** to another computer.

By default the `drwinst` instruction launched without parameters will scan the network for **Dr.Web Servers** and will try to install **Agent** from the first found **Server** (the *Multicasting* mode with using Server Detection Service).

Thus, the **Server** address become known for the **Agent** during installation.

You can change the **Server** address in the **Agent** settings manually later.

3.2.2. Dr.Web Server Detection Service

In this connection scheme, client does not know the **Server** address preliminary. Before establishing each connection, the **Server** will be searched in the network. To do this, the client sends the broadcast query and waits for the respond, that includes **Server** address. After the client gets respond, it will establish a connection with the **Server**.

To realize this scheme, the **Server** must "listen" the network for such queries.

Several variants of realization of this scheme is available. Most important is that the **Server** search method at the clients side must be matched with the **Server** respond part.

The *Multicast over UDP* mode is used by default in the **Dr.Web Enterprise Security Suite**:

1. **Server** gets registered in the multicast group with an address specified in the **Server** settings.
2. **Agents** during **Server** search, send multicast requests to the group address specified at the step 1.

Server listens by default (similarly to direct connections):

- `udp/231.0.0.1:2193`

Note: in **Servers** v. **4.XX** the `2371` port was used. In the **10.0** version this port is no longer supported.

This parameter is set at the **Servers** settings: **Administration** → **Dr.Web Server configuration** → **Transport** tab → **Multicast group** field.

3.2.3. Using SRV Protocol

Clients under Windows OS support *SRV* client network protocol (format description is given in the **Appendices** document, p. Appendix E. The Specification of Network Addresses).

Accessing the **Server** via the SRV records are implemented by the following way:

1. During the **Server** installation, registration in Active Directory domain is set up, installer registers corresponding SRV record on DNS server.

SRV record is registered on DNS server according to the RFC2782 (see http://tools.ietf.org/html/rfc2782).

2. In a request for connecting the **Server**, client specifies access via the `srv` protocol.

   For example, launch the **Agent** installer with explicit specification of the **Server** looks as following:

   ```
   drwinst srv/drwcs
   ```

3. Transparently for the user, the client uses functional of SRV protocol to access to the **Server**.

If the **Server** is not specified directly, the `drwcs` is used by default as a name of the service.

Chapter 4: Anti-Virus Network Administrators

It is recommended to appoint a reliable, qualified employer experienced in the administration of a local network and competent in anti-virus protection as an administrator of the anti-virus network. Such employer should have full access to the installation folders of **Dr.Web Server**. Depending on organization security policy and staffing situation, such employer should either be a local network administrator or work closely with such person.

To manage the anti-virus network, it is not necessary to have administrator rights on computers included in the anti-virus network. However, remote installation and removal of the **Agent** software is possible within a local network only and requires administrator's rights in the local network, and checkout of **Dr.Web Server** requires full access to its installation folder.

4.1. Authentication of Administrators

To connect to Dr.Web Server, administrator can authenticate by the following ways:

1. With storing administrative account information in the **Server** DB.
2. Via the Active Directory (for **Servers** under Windows OS).
3. Via the LDAP protocol.
4. Via the RADIUS protocol.
5. Via PAM (only for UNIX system-based OS).

Authentication methods are used sequentially according to the following rules:

1. The order of authentication methods usage depends on the order of their following in the settings, specified in the **Control Center**.
2. Authentication of administrator from the **Server** DB is always tried first.
3. By default, LDAP authentication is used by the second, via the Active Directory - the third, via the RADIUS - the fourth. Under UNIX system-based OS, the PAM is used the fifth.
4. Authentication methods via LDAP, Active Directory and RADIUS can be swapped in the **Server** settings, but authentication of administrator from the **Server** DB is always used first.
5. Authentication methods via LDAP, Active Directory and RADIUS are disabled by default.

To swap the usage of authentication methods:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authentication** in the control menu.
3. In the opened window, list of authentications types is represented in the order of use. To change this order, drag and drop authentication methods in the list and place them in the necessary order of use the authentication.
4. To apply changes, you must restart the **Server**.

Administrative login must be unique.

Administrators are not allowed to connect via external authentication systems if an administrator with the same login already exists at the **Server**.

4.1.1. Authentication of Administrators from the Server DB

Authentication method with storing administrative account information in the **Server** DB is used by default.

To manage administrators list:

1. Select **Adminiatration** in the main menu of the **Control Center**.
2. Select **Administrators** in the control menu. The list of all administrators registered in the DB will be opened.

   See the Administrators and Administrative groups section for details.

4.1.2. Active Directory Authentication

To enable Active Directory authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authentication** in the control menu.
3. In the opened window, select **Microsoft Active Directory** section.
4. Set the **Use Microsoft Active Directory authentication** flag.
5. Click **Save**.
6. Restart the **Server** to apply changes.

For Active Directory authentication, only enabling of using this authentication method is configured in **Control Center**.

You must edit Active Directory administrators' settings manually at the Active Directory server.

To edit Active Directory administrators:

The following operation must be carried out from a computer with Active Directory Service snap-in.

1. To enable editing of administrator parameters, do the following:
   a) Modify the Active Directory scheme with the `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxx-windows-nt-xYY.exe` utility (it is included into **Dr.Web Server** distribution kit).
   Modification of Active Directory scheme may take some time. Depending on the domain configuration, it may take up to 5 minutes and more to synchronize and apply the modified scheme.

If the Active Directory scheme has been modified earlier via this utility for the **6** version of the **Server**, it is no need to perform modification repeatedly via the utility from the **10.0** version of the **Server**.

   b) Register Active Directory Schema snap-in, execute the `regsvr32 schmmgmt.dll` command with the administrative privileges, then run `mmc` and add the **Active Directory Schema** snap-in.
   c) Using the Active Directory Schema snap-in, add the auxiliary **DrWebEnterpriseUser** class to the **User** and (if necessary) **Group** classes.

If the scheme modification and application process has not finished, the **DrWebEnterpriseUser** class may be not found. In this case, wait for a few minutes and retry to add the class as described in **c)** step.

d) With the administrative privileges run the `drweb-esuite-aduac-xxxxxxxxxxxxxx-windows-nt-xYY.msi` file (is included in the **Enterprise Security Suite 10.0** distribution kit) and wait until the installation finishes.

2. Visual editing of attributes is available from the **Active Directory Users and Computers** control panel → **Users** section → in the **Administrator Properties** window for editing settings of selected user → on the **Dr.Web Authentication** tab.
3. The following parameter is available for editing (**yes**, **no** or **not set** values can be set for the attribute):
   - **User is administrator** indicates that the user is full-rights administrator.

Algorithms of operating principles and attributes handling during authentication are described in the **Appendices** document, in the Appendix C1 section.

4.1.3. LDAP Authentication

To enable LDAP authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authentication** in the control menu.
3. In the opened window, select **LDAP authentication** section.
4. Set the **Use LDAP authentication** flag.
5. Click **Save**.
6. Restart the **Server** to apply changes.

You can configure authentication using LDAP protocol at any LDAP server. Also you can use this mechanism to configure the **Server** under UNIX system-based OS for authentication in Active Directory on a domain controller.

Settings of LDAP authentication are stored in the `auth-ldap.xml` configuration file.

General xml attributes are described in the **Appendices** document, in the Appendix C2 section.

Unlike to Active Directory, this mechanism can be configures to any LDAP scheme. By default **Server** attributes are used as they were defined for Active Directory.

LDAP authentication process can be presented as the following:

1. LDAP server address is specified via the **Control Center** or xml configuration file.
2. For the specified user name, the following actions are performed:
   - Translation of name to the DN (Distinguished Name) using DOS-like masks (with * symbol), if rules are specified.
   - Translation of name to the DN using regular expressions, if rules are specified.
   - Custom script for translation of name to the DN is used, if it is specified in settings.
   - If matches in translation rules are not found, specified name is used as it is.

Format of user names specifying is not predefined and not fixed - it can be any as it is accepted in the company, i.e. forced modification of LDAP scheme is not demanded. Translation according given scheme is performed using rules of translation of names to LDAP DN.

3. After translation, like for the Active Directory, attempt of the user registration at the specified LDAP server using determined DN and specified password is performed.
4. After this, like for the Active Directory, LDAP object attributes are read for the determined DN. Attributes and their possible values can be redefined in the configuration file.
5. If undefined values of administrator attributes are found, and inheriting is specified (in the configuration file), the search of needed attributes in the user groups is the same as in the Active Directory.

4.1.4. RADIUS Authentication

To enable RADIUS authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authentication** in the control menu.
3. In the opened window, select **RADIUS authentication** section.
4. Set the **Use RADIUS authentication** flag.
5. Click **Save**.
6. Restart the **Server** to apply changes.

To use the RADIUS authentication and authentication protocol, you must install a server that implements this protocol, e.g., freeradius (for more details, see http://freeradius.org/).

In the **Control Center** you can specify the following parameters for the RADIUS server communication:

- **Server**, **Port**, **Password** - parameters for connection to the RADIUS server: IP address/DNS name, port number, password (secret) correspondingly.
- **Timeout** - time for waiting the response from the RADIUS server, in seconds.
- **Retries number** - maximum number of retries to connect the RADIUS server.

Also, you can setup additional RADIUS parameters via the following tools:

- The `auth-radius.xml` configuration file located in the `etc` folder of the **Server**.

  Besides parameters that are specified via the **Control Center**, in the configuration file you can specify the NAS identifier value. This identifier according to the RFC 2865, can be used instead of IP address/ DNS name as a client's identifier for connection to the RADIUS server. In the configuration file it is stored in the following form:

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

- The `dictionary.drweb` dictionary located in the `etc` folder of the **Server**.

  The dictionary stores the list of RADIUS attributes of **Doctor Web** company (VSA - Vendor-Specific Attributes).

4.1.5. PAM Authentication

To enable PAM authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authentication** in the control menu.
3. In the opened window, select **PAM authentication** section.
4. Set the **Use PAM authentication** flag.
5. Click **Save**.
6. Restart the **Server** to apply changes.

PAM authentication under UNIX system-based OS is performed by using pluggable authentication modules.

To configure PAM authentication parameters, you can use one of the following ways:

- Configure authentication methods via the **Control Center**: in the **Administration** → **Authentication** → **PAM authentication** section.
- The `auth-pam.xml` configuration file located in the `etc` folder of the **Server**. Configuration file example is:

```
...
<!-- Enable this authorization module -->
  <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
  <admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />
...
```

Description of PAM authentication parameters which are configured at Dr.Web Enterprise Security Suite side

Control Center items	auth-pam.xml file items			Description
	Block	Para-meter	Available values	
Use PAM authentication flag	`<enabled>`	`value`	yes | no	Flag that defines whether the PAM authentication method is used.
Use *Drag and Drop*	`<order>`	`value`	positive integer, coordinated with other methods values	Serial number of PAM authentication if several authentication methods are used.
Service name field	`<service>`	`name`	-	Service name which is used to create PAM context. PAM can read politics for this service from the `/etc/pam.d/<service name>` or from the `/etc/pam.conf`, if the file does not exist. If the parameter is not set (no `<service>` tag in the configuration file), the `drwcs` name is used by default.
Control flag is mandatory flag	`<admin-flag>`	`mandatory`	yes | no	Parameter defines whether the control flag identifying a user as an administrator is mandatory. By default is `yes`.

Control Center items	auth-pam.xml file items			Description
	Block	Para-meter	Available values	
Control flag name field	<admin-flag>	name	-	Key string according to which PAM modules read the flag. By default is `DrWeb_ESuite_Admin`.

When configuring operating of PAM authentication modules, use parameters which are set at **Dr.Web Enterprise Security Suite** side, and consider default values which are used if parameters are not specified.

4.2. Administrators and Administrative groups

To open administrative accounts control section, select **Administration** in the main menu of the **Control Center** and then in the opened window select the **Administrators** item of the control menu.

The **Administrators** section is available for all **Control Center** administrators. Full hierarchical tree of administrators is available only for **Administrators** group members who have the **View properties and configuration of administrative groups** permission. The rest of administrators will only see their respective groups with subgroups and accounts.

Hierarchy of Administrators

Hierarchical view of administrators is a tree which represents a structure of administrative groups and administrators accounts. Administrative groups and their members (administrators accounts) both can be nodes of such tree. Each administrator can be a member of only one group. Nesting level of groups in a tree is not limited.

Predefined groups

After installing **Dr.Web Server** two groups are automatically created:

- **Administrators**. The group initially contains only **admin** user with a full set of privileges. The **admin** user is automatically created during **Dr.Web Server** installation (see below).
- **Newbies**. The group is initially empty. Administrators with external type of authentication, such as LDAP, Active Directory or RADIUS, will be automatically moved to this group.

  Administrators of the **Newbies** group have read-only access by default.

Predefined administrators

After installing **Dr.Web Server** the following administrative account is automatically created:

Parameter	Value
Account name	**admin**
Password	Password is set during **Dr.Web Server** installation (step 15 of installation procedure).
Privileges	Full set of privileges.
Account editing	Administrator privileges cannot be edited. Administrative account cannot be deleted.

Hierarchical Lists Displaying

- In the hierarchical list of anti-virus network: administrator sees only those user groups, which are granted in the **View groups of stations properties** permission. All system groups are also displayed in the anti-virus network tree, but only stations from the specified user groups list are available inside.
- In the hierarchical list of administrators: administrator from the **Newbies** group sees only a tree, the root node of which is a group of this administrator, i.e. sees administrators from the own group and its subgroups. Administrator from the **Administrators** group sees all administrators not depending on their groups.

Administrators Permissions

All administrators activity in **Control Center** depends on the set of permissions, which can be defined either for specific account or for a group of administrators.

Administrative permissions system includes the following opportunities of permissions management:

- **Granting permissions**

  Granting permissions performed during creation of administrative account or administrative group. When administrator or administrative account is created, it inherits permissions from the parent group it is added to. Changing permissions is not allowed during creation.

- **Inheriting permissions**

  By default permissions of administrators and administrative groups are inherited from respective parent groups, but this behavior can be changed.

  It is possible to define a custom set of permissions for a specific administrative account while the rest permissions will continue to be inherited from account parent group. Inheriting account or group permissions does not reassign them from parent to a child but calculates new set of privileges from permissions of all parent groups in the branch of hierarchy. The resulting set of permissions for an object depends on inheriting and parent groups permissions can be found in the **Appendices** document, in the Appendix C3 section.

- **Changing permissions**

  Changing permissions is not allowed for administrators accounts or administrative groups during creation. Permissions can be changed only for already created accounts and groups and can be done in the properties section of an account or a group. You can only reduce permissions at editing. You cannot edit permissions for the **admin** predefined administrator.

  The procedure is described in the Editing Administrative Accounts and Groups section.

Brief description of administrative permissions and **Control Center** sections depended on a certain permissions, is given in the **Appendices** document, in the Appendix C4. section.

4.3. Management of Administrative Accounts and Administrative Groups

4.3.1. Creating and Deleting Administrative Accounts and Groups

Administrative login must be unique.

Administrators are not allowed to connect via external authentication systems if an administrator with the same login already exists at the **Server**.

Adding Administrators

To create administrative account, administrator must have **Create administrators, administrative groups** permission.

To add a new administrative account:

1. Select the **Administration** item in the main menu of **Dr.Web Security Control Center** and in the opened windows, select the **Administrators** item in the control menu.
2. Click the **Create account** icon in the toolbar. A window with creating account settings will be opened.
3. In the **General** section, specify the following parameters:
   - In the **Login** field specify administrator account login for **Dr.Web Security Control Center** access. It is allowed to use lower case characters (a-z), upper case characters (A-Z), digits (0-9), symbols "_" and ".".
   - In the **Authentication type** list, select one on the following variants:
     - **Internal** - authentication of such administrator in the **Control Center** is based on the credentials in the DB of **Dr.Web Server**.
     - **External** - authentication of such administrator in the **Control Center** is performed via LDAP, Active Directory, RADIUS or PAM external systems.

For more details see Authentication of Administrators.

   - In the **Password** and **Retype password** fields set the password for accessing the **Server** and **Dr.Web Security Control Center**.

It is not allowed to use national characters in administrator password.

   - In the **First name**, **Middle name** and **Last name** fields you can specify administrator's personal data.
   - In the **Interface language** drop-down list, select the language which will be used by the adding administrator (web browser language or English is specified by default).
   - In the **Date format** drop-down list, select the date format which will be used by this administrator during editing settings that contain dates. The following formats are available:
     - European: `DD-MM-YYYY HH:MM:SS`
     - American: `MM/DD/YYYY HH:MM:SS`

- In the **Description** field, you can set optional description of the account.

Values of fields, marked by the * sign, must be obligatory specified.

4. In the **Groups** subsection, you can specify parental administrative group. The list contains groups to which an administrator can be assigned. The flag is set next to the group to which created administrator will be assigned. Created administrators are placed in the parent group of current administrator by default. To change specified group, set the flag next to the required group.

   Each administrator may be a member of one group only.

   Administrator inherits permissions from the parental group (see Administrators and Administrative groups).

5. After you set all necessary parameters, click **Save** to create a new administrative account.

Adding Administrative Groups

To create administrative groups, administrator must have **Create administrators, administrative groups** permission.

To add a new administrative group:

1. Select the **Administration** item in the main menu of **Dr.Web Security Control Center** and in the opened windows, select the **Administrators** item in the control menu.
2. Click the **Create group** icon in the toolbar. A window with creating group settings will be opened.
3. In the **General** section, specify the following parameters:
   - In the **Group field**, specify the name of administrative group. It is allowed to use lower case characters (a-z), upper case characters (A-Z), digits (0-9), symbols "_" and ".".
   - In the **Description** field, you can set optional description of the group.
4. In the **Groups** subsection, you can specify parental administrative group. The list contains groups which can be assigned as a parental group. The flag is set next to the group into which created administrative group will be included. Created groups are placed in the parent group of current administrator by default. To change specified group, set the flag next to the required group.

   Only one parent group can be assigned.

   Administrative group inherits permissions from the parental group (see Administrators and Administrative groups).

5. After you set all necessary parameters, click **Save** to create a new administrative group.

Deleting Administrators and Administrative Groups

To delete administrative accounts and administrative groups, administrator must have **Create administrators, administrative groups** and **Edit properties and configuration of administrative groups** permissions correspondingly.

To delete administrator account:

1. Select the **Administration** item in the main menu of **Dr.Web Security Control Center** and then the **Administrators** item in the control menu.

2. In the administrators hierarchical list, select administrative account or administrative group you want to delete.
3. Click the **Remove selected objects** icon in the toolbar.

4.3.2. Editing Administrative Accounts and Groups

To edit accounts of administrators and administrative groups, you need to have the **Editing administrative accounts** and **Editing administrative group configuration properties privileges** permissions.

Fields marked with the * sign must be specified.

Editing Administrators

To edit an administrative account:

1. Select the account you want to edit from the list of administrative accounts. Click the account name to open its properties section for editing.
2. The **Main** subsection contains properties that were set during account creation. Also, please note:

a) To change the password for the administrative account, click the **Change password** icon on the toolbar.

An administrator with corresponding permissions can change passwords of all other administrators.

Login for administrative account cannot contain national characters.

b) The following properties of the administrator account are read-only:

- Account creation date and its properties last change date,
- **Status** - displays network address of the last connection under the current account.

3. In the **Groups** subsection, you can change an administrative group. The list contains groups to which an administrator can be assigned. The flag is set next to the current parent group of administrator. To change assigned group, set the flag next to the required group.

   It is mandatory to assign a parent group to the administrator. Each administrator can be included only to the one group at a time. Permissions of administrator are inherited from the parent group.

   See also the Editing membership subsection.

4. In the **Permissions** subsection, you can edit the list of actions that are allowed for the administrator.

   Details on editing permissions are described in the Editing permissions subsection.

5. Click **Save** to apply changes.

Editing Administrative Groups

To edit an administrative group:

1. Select the group you want to edit from the list of the administrators. Click the group name to open its properties section for editing.
2. The **Main** subsection contains properties that were set during group creation.
3. In the **Groups** subsection you can change the parent administrative group. The list contains groups which can be assigned as a parental group. The flag is set next to the current parent group. To change assigned group, set the flag next to the required group.

   It is mandatory to assign a parent group to the administrative group. The group inherits permissions from its parent group.

   See also the Editing membership subsection.

4. In the **Permissions** subsection, you can edit the list of allowed actions.

   Details on editing permissions are described in the Editing permissions subsection.

6. Click **Save** to apply changes.

Editing Permissions

To edit privileges of administrators and administrative groups in the properties editing section:

1. To change the inheritance, click **on/off** in the **Inheritance** column of the permissions table and select the necessary value in the drop-down list.
2. The list of permissions is divided into three subsections:
   - permissions for managing stations/groups of stations,
   - permissions for managing administrators/administrative groups,
   - permissions with flags.
3. Permissions of the first two sections are managed in the **Granted** and **Denied** columns.

   These permissions are applied according to the following rules:

Cell content	Value in column	
	Granted	Denied
Group name or list of the group names	Permission is allowed only for the listed groups	Permission is denied only for the listed groups
All	Permission is allowed for all groups	Permission is denied for all groups
None	Permission is not allowed for any group	Permission is not denied for any group

To edit a permission, click on a respective cell. A window with a list of groups that are affected by the permission will be opened. Select one of the two available settings from the list:

Setting name	Action on the setting specifying
For stations	
All	Apply permission settings for all stations that are connected to the current **Server**.

Setting name	Action on the setting specifying
Select certain stations	Apply permission settings only for the stations in the selected groups. To assign certain group, single-click it in the **Anti-virus network** list. To select multiple groups, press the CTRL or the SHIFT key.
For administrators	
All	Apply permission settings for all administrators of the current **Server**.
Select certain administrators	Apply permission settings only for the administrators in the selected administrative groups. To assign certain group, single-click it in the **Administrators** list. To select multiple groups, press the CTRL or the SHIFT key.

4. To manage permissions from the third section, set a flag next to respective permission either in the **Granted** or **Denied** column: to correspondingly allow or deny this permission for the administrators of editing group.
5. Click **Save** to apply changes.

Editing Membership

There are several ways to assign a parent group for an administrator or an administrative group:

1. Change administrator settings or group settings as described above.
2. Drag-and-drop administrator or administrative group from the hierarchical tree to the group you want to assign as a parent group.

Chapter 5: Groups. Integrated Workstations Management

Grouping is designed to make the administration of anti-virus workstations easier.

Grouping of stations may be used for the following purposes:

- Group operations over all stations, included to these groups.

  As for separate group so and for several selected groups, you can launch, view and stop scan tasks on stations, included to this group. In the same way, you can view statistics (including infections, viruses, start/stop, scan and installation errors and etc) and summary statistic for all workstations of the group or several groups.

- Settings the single parameters for stations via the group, to which these stations are included (see p. Using Groups to Configure Stations).
- Order (structure) the list of workstations.

It is possible to create nested groups.

5.1. System and User Groups

System Groups

Dr.Web Enterprise Security Suite has an initial set of preinstalled system groups. These groups are created during the installation of **Dr.Web Server** and may not be deleted. Still the administrator may disable their display, if necessary.

Each system group except **Everyone** contains a set of feature-packed subgroups.

After the **Server** has been installed, until no station connected, the list of system groups displays the **Everyone** group only. To display all system groups, use the **Show hidden groups** option in the **Settings of tree view** section of the toolbar.

Everyone group

Group contains all stations known to **Dr.Web Server**. The **Everyone** group has default settings.

Configured

Group contains stations which have personal settings specified.

Operating system

This category of groups represents the operating systems under which the stations are working at the moment. These groups are not virtual, may have station settings and be primary groups.

- **Android** family groups. This family includes a set of groups, that correspond to specific version of Android OS for mobile devices.
- **Mac OS X** family groups. This family includes a set of groups, that correspond to specific version of OS X operating system.
- **Netware** group. This group contains stations, that operate under Novell NetWare OS.

- **UNIX** family groups. This family includes a set of groups, that correspond to OS of UNIX system-based systems, for example, Linux, FreeBSD, Solaris, etc.
- **Windows** family groups. This family includes a set of groups, that correspond to specific version of Windows operating system.

Status

The **Status** group contains subgroups reflect the current status of the station, that is if it is connected to the **Server** or not at the moment. These groups are completely virtual, may not have any settings or be primary groups.

- **Deinstalled** group. Once **Dr.Web Agent** software has been deinstalled from a station, the station is transferred to the **Deinstalled** group.
- **Deleted** group. Contains stations, which were deleted by an administrator from the **Server**. Such stations can be restored (see p. Removing and Restoring Stations).
- **New** group. Contains new stations, which have been created by administrator via **Dr.Web Security Control Center**, but the **Agent** is not installed yet.
- **Newbies** group. Contains all unapproved stations not registered at the **Server** at the moment. When the registration is approved or access to the **Server** is denied, stations will be removed from this group automatically.
- **Offline** group. Contains all workstations not connected at the moment.
- **Online** group. Contains all workstations connected at the moment (reacting to **Server** requests).
- **Update Errors** group. Contains all workstations that have been failed to update.

Transport

The following subgroups elicit the protocol of workstations connection to the **Server**. These groups are completely virtual, may not have any settings or be primary groups.

- **TCP/IP** group. The group contains workstations connected at the moment through the TCP/IP protocol.
- **TCP/IP Version 6** group. The group contains workstations connected at the moment through the TCP/IP version 6 protocol.

Ungrouped

Group contains stations, which are not included in any of user groups.

User Groups

These groups are assigned by the anti-virus network administrator for his/her own needs. The administrator may create own groups and include workstations in them. The contents and names of such groups are not restricted by **Dr.Web Enterprise Security Suite** in any manner.

In the table 5-1, all possible groups and group types are given for your reference, along with the specific parameters supported (+) or not supported (–) by the groups.

The following parameters are considered:

- **Automatic membership**. The parameter reflects whether stations may be automatically included in the group (automatic membership support) and group contents automatically adjusted during **Server** operation.
- **Membership administration**. The parameter reflects whether the administrator can manage group membership: add stations to or remove from the group.

- **Primary group**. The parameter reflects whether the group can be primary for a station.
- **Possibility to have own settings**. The parameter reflects whether the group can have own settings of anti-virus components (to be propagated to its stations).

Table 5-1. Groups and supported parameters

Group/group type	Parameter			
	Automatic membership	Membership administration	Primary group	Possibility to have own settings
Everyone	+	–	+	+
Configured	+	–	–	–
Operating system	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–
User groups	–	+	+	+

Under group administrator account, the user group which he manages will be the root of the hierarchical tree, even if it has the parent group. All nested groups of managing group is available.

5.2. Group Management

5.2.1. Creating and Deleting Groups

Creating Groups

To create a new group:

1. Select: **Add a station or a group** on the toolbar and the **Create group** in the submenu. A window for creating a group will be opened.
2. The **Identifier** field is filled automatically. You can edit it during creation, if necessary. The identifier should not contain spaces. In the sequel group identifier can not be changed.
3. Specify the group name in the **Name** field.
4. For nested groups, in the **Parent group** field, select from the drop-down list a parental group to inherit configuration from it if personal settings are not specified. For a root group (without a parent), leave this field blank to add the group to the root of the hierarchical tree. In this case settings are inherited from the **Everyone** group.
5. Specify optional comment in the **Description** field.Click **Save**.

The groups you create are initially empty. Procedure of including workstations to groups is described in the Including Workstations into User Groups section.

Deleting Groups

To delete existing group:

1. Select the user group in the hierarchical list of the **Control Center**.
2. Click **General** → **Remove selected objects** on the toolbar.

You cannot delete preinstalled groups.

5.2.2. Editing Groups

To edit group properties:

1. Select the **Anti-virus network** item in the main menu of **Dr.Web Security Control Center**, then select the group in the hierarchical list of the opened window.
2. Open the group properties section by one of the following ways:
   a) Click the name of the group in the hierarchical list of anti-virus network. A panel with properties of the group will be automatically opened in the right part of **Dr.Web Security Control Center**.
   b) Click **Properties** in the control menu. A window with the group properties will be opened.
3. Window with the group settings contains the **General** and **Configuration** sections. These settings are described below.

If you open group properties in the right part of the **Control Center** (see the step **2.a)**), the **Stations information** section with general information about stations, included to this group, will be also available.

4. Click **Save** to save all changes.

General

In the **General** section, the following information is presented:

- **ID** - group unique identifier. Is read-only.
- **Name** - group name. You can change the group name, if necessary. For preinstalled groups, the **Name** field is read-only.
- **Parent group** - parent group in which this group is included and from which group configuration is inherited, if the personal settings are not specified. If a parent group is not specified, settings are inherited from the **Everyone** group.
- **Description** - optional filed with group description.

Stations Information

In the **Stations information** section, the following information is presented:

- **Stations** - total number of stations which are included into this group.
- **Primary group for** - number of stations for which this group is primary.
- **Stations online** - number of stations in this group which are currently online.

Configuration

For more details on inheriting of group settings by stations, for which this group is primary, see the Using Groups to Configure Stations section.

In the **Configuration** section, the following groups parameters are presented:

Icon	Settings	Description section
	Permissions for workstations, which inherit this setting from a group if it is primary. Setting permissions of groups is similar to setting permissions of separate workstations.	Permissions of Station Users
	Centralized task schedule for workstations, which inherit this setting from a group if it is primary. Setting schedule of group is similar to setting centralized schedule of separate workstations.	Scheduled Tasks of a Station
	License key file for workstations, which inherit this setting from a group if it is primary.	License Manager
	Restrictions for anti-virus software updating for workstations, which inherit this setting from a group if it is primary.	Update Restrictions for Workstations
	Installing components list for workstations, which inherit this setting from a group if it is a primary. Editing the components list of group is similar to setting the components list of separate stations.	Installing Components of the Anti-Virus Package
	Configuring automatic placing the stations into the group. Available for user groups only.	Configuring Automatic Group Membership
	Settings of the anti-virus components. Setting the anti-virus package components of group is similar to setting the anti-virus package components of separate workstations.	Management of Anti-virus Components

5.3. Including Workstations into User Groups

Dr.Web Enterprise Security Suite provides the following ways how to place stations into user groups:

1. Place stations into groups manually.
2. Use automatic group membership.

5.3.1. Including Stations into Groups Manually

There are several ways how to add a workstation to a user group manually:

1. Change the station settings.
2. Drag-and-drop a station in the hierarchical list.

To edit the list of groups containing the station via the station settings:

1. In the main menu, select **Anti-virus network**, then click the name of a workstation in the hierarchical list.
2. The station properties panel opens. Also, you can open the stations properties section by selecting **Properties** in the control menu.
3. In the **Station Properties** pane, select the **Groups** section.

   The **Membership** list displays the groups which include the workstation and to which you can include it.
4. To add the workstation into a group, set the flag for this group in the **Membership** list.
5. To remove a workstation from the group, clear the flag for this group in the **Membership** list.

You cannot remove stations from preinstalled groups.

6. To save changed settings, click **Save**.

In the **Properties** section, you can also set a group as a primary one for the station (for more details, read p. Inheriting Stations Configuration from Groups. Primary Groups).

To edit the list of groups containing the station via the hierarchical list:

1. In the main menu, select **Anti-virus network** and unfold the hierarchical list of groups and stations.
2. To add a station to the user group, press CTRL and drag-and-drop a station to the corresponding group.
3. To move a station from one user group to another, drag-and-drop this station from the user group, from which station will be removed, to the user group, to which station will be added.

When dragging a station from preinstalled group in both 2 and 3 steps, station is added in the user group and is not removed from preinstalled group.

5.3.2. Configuring Automatic Group Membership

Dr.Web Enterprise Security Suite allows to configure the rules of automatic including stations into user groups.

To specify the rules of automatic including stations into the group:

1. Select the **Anti-virus Network** item in the main menu of the **Control Center**.
2. In the hierarchical list of anti-virus network, select the user group for which you want to specify the membership rules.
3. Open the membership rules editing section by one of the following ways:
   - In the group properties pane on the right part of the window, in the **Configuration** section, click **Group membership rules**.
   - In the control menu, in the **General** section, select the **Group membership rules** item.
   - In the control menu, in the **General** section, select the **Properties** item, open the **Configuration** tab and click **Group membership rules**.
4. In the opened window, specify the conditions under which stations will be included into this group:
   a) If the group membership rules have not been specified before, click **Add the rule**.
   b) For each block of rules, specify the following settings:
      - Select one of the options that sets the mode of rules combination inside this block: **Matches all conditions**, **Matches any of conditions**, **Does not match any of conditions**.
      - In the conditions drop-down lists, select: one of the station parameters that will be checked for compliance with the conditions; the mode of correspondence with this condition and specify the condition string if the station parameter assumes it.
      - To add one more condition in this block of rules, click from the right of condition string.
   c) To add a new block of rules, click from the right of the block. At this, specify the mode of integration of this block of conditions with other blocks:
      - **AND** - conditions of blocks must be carried simultaneously.
      - **OR** - conditions at least one of the blocks must be carried out.

To specify the condition string, you may use regular expressions.

Regular expressions briefly described in the **Appendices** document, in the Appendix J. Regular Expressions Used in Dr.Web Enterprise Security Suite section.

Please note: for the **starts with** and **ends with** filter parameters, the condition string is automatically complemented with the following escape characters correspondingly: ^ (string starts with the specified symbols) or $ (string ends with the specified symbols).

For fully usage of regular expressions, it is recommended to select the **contains** filter parameter.

5. To save and apply the specified rules, click one of the following buttons:
   - **Apply now** - save the specified membership rules and apply these rules immediately to all stations registered on this **Server**. If a lot of stations are registered on the **Server**, execution of this action may take some time. Rules of stations regrouping are applied to all already registered stations immediately after the action is set and will be applied further to all stations, including the firstly registered on the **Server**, at the moment of their connection.
   - **Apply on stations connect** - save the specified membership rules and apply these rules to stations in the moment of their connection to the **Server**. Rules of stations regrouping are applied to all already registered stations at the moment of their next connection to the **Server** and will be applied to all stations firstly registered on the **Server** at the moment of their first connection.
6. When automatic membership rules are specified for a user group, next to the icon of this group in the hierarchical list, the icon displays, if the **Show membership rules icon** flag is set in the **Settings of tree view** list on the toolbar.

If the station was automatically included into the user group according to the membership rules, when removing the station from this groups manually makes no sense, because the station will be automatically returned to this group at the next connection to the **Server**.

To remove the rules of automatic including stations into the group:

1. Select the **Anti-virus Network** item in the main menu of the **Control Center**.
2. In the hierarchical list of anti-virus network, select a user group for which you want to remove the membership rules.
3. Perform one of the following actions:
   - On the toolbar, click **Remove membership rules**.
   - In the group properties pane on the right part of the window, in the **Configuration** section, click **Remove membership rules**.
   - In the control menu, in the **General** section, select the **Properties** item, open the **Configuration** tab and click **Remove membership rules**.
4. After group membership rules are removed, all stations that have been included into this group automatically will be removed from this group. If for any of automatically included stations, this group was set by administrator as primary, after removing stations from the group, the **Everyone** group will be set as primary for these stations.

5.4. Using Groups to Configure Stations

Stations settings can be:

1. Inherited from the primary group.
2. Specified personally.

Inherited Settings

For created group, its settings are inherited from the parental group or from the **Everyone** group, if the parental group is not specified.

For created station, its settings are inherited for the primary group.

For more details, see the Inheriting Stations Configuration from Groups. Primary Groups section.

When viewing or editing workstation configuration inherited from the primary group, a notification that the settings are inherited from the primary group will be displayed in correspondent windows.

You can set different configurations for different groups and stations, by editing corresponding settings.

Personal Settings

To set the personal settings for the station, edit corresponding settings section (see p. Management of Stations Configuration). In the settings section, notification that the settings are set personally for the station will be displayed.

If the personal settings are specified for the station, personal group settings and their changing will not have any affect on station settings.

You can restore the configuration inherited from the primary group. To do this, click the **Remove personal settings** button in the toolbar of **Dr.Web Security Control Center**, in the corresponding parameters section or in the station settings section.

5.4.1. Inheriting Stations Configuration from Groups. Primary Groups

Inheriting a Station Settings

When a new workstation is created, its configuration settings are inherited from one of the groups to which the station is included. That group is called a *primary group*.If the settings of the primary group are modified, these changes are inherited by all workstations included into the group, unless the workstations have been customized. When creating a workstation, you can specify what group will be regarded as primary. By default the primary group is **Everyone**.

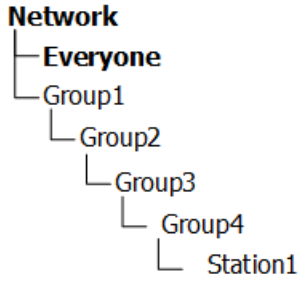
If **Everyone** is not a primary group, and a different primary group has no personal settings, the settings of the **Everyone** group are inherited by a new station.

It is possible to create nested groups.

Inheritance in nested groups depends on groups hierarchy. If a station have no personal settings, it inherits the configuration from a parent group, and this process repeats recursively. Therefore the search for group configuration is performed upwards through the hierarchical tree of nested groups, starting from the station primary group and till the root group. If no personal settings are selected for all nesting groups, then the **Everyone** group settings are inherited.

Example

The structure of hierarchical list is the following:



The `Group4` is the primary group for the `Station1`. To determine which settings to inherit for the `Station1`, the search is carried out in the following order: `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

By default the network structure is displayed in such a way as to show a station in all the groups it is included into. If you want workstations to be displayed in the network catalog in their primary groups only, on the toolbar in **Settings of tree view**, clear the **All groups membership** flag.

Setting a Primary Group

There are several ways how to set a new primary group for a workstation or a group of workstations.

To set primary group for station

1. In the main menu, select **Anti-virus network**, then click the name of a workstation in the hierarchical list.
2. The station properties panel opens. Also, you can open the stations properties section by selecting **Properties** in the control menu. In the opened window, go the **Groups** section.
3. If you want to reassign the other primary group, click an icon of necessary group in the **Membership** list. The **1** sign displays on the icon.
4. Click **Save**.

To set primary group for several stations

1. In the main menu, select **Anti-virus network**. In the hierarchical list of the opened window, click the name of workstations (you can select groups of workstations either, in such case, the action spreads on all stations in the group) for which you want to set a primary group. To select several workstations and groups, press and hold CTRL or SHIFT during mouse selection.
2. On the toolbar, click **General** → **Set a primary group for stations**. This opens the window listing the groups which can be set as primary for the selected workstations.
3. Click the name of a group to set it as primary.

You can also make a group primary for all workstations included into it. To do this, select the necessary group in the hierarchical list, and click **General** → **Set this group as primary** on the toolbar.

5.4.2. Propagation of Settings to Other Groups/Stations

Configuration settings of anti-virus programs, schedules and user permissions and other settings of a group or a workstation can be copied (propagated) to other group or several groups and workstations.

To propagate settings:

1. Click **Propagate these settings to another object** in the one of the following locations:
   - in the editor of anti-virus component configuration,
   - in the schedule editor,
   - in the update restrictions window,
   - in the installing components window,
   - in the window for stations user permissions setup.

   A window of the anti-virus network hierarchical list will be opened.
2. Select necessary groups and stations to which you want to propagate the settings.
3. To enable changes in the configuration of these groups, click **Save**.

5.5. Comparison of Stations and Groups

You can compare stations and groups by general parameters.

To compare several objects of the anti-virus network:

1. In the main menu, select **Anti-virus network**, then select the objects you want to compare in the hierarchical list. Use CTRL and SHIFT for this. The following variants are possible:
   - selection of several stations - to compare selected stations;
   - selection of several groups - to compare selected groups and all nested groups;
   - selection of several stations and groups - to compare all stations: selected directly in the hierarchical list and included in all groups and their nested groups.
2. In the control menu, click **Comparison**.
3. The comparison table for selected objects will be opened.
   - Comparative parameters for groups:
     - **Stations** - total number of stations, included in this group.
     - **Stations online** - number of on-line stations.
     - **Primary group for** - number of stations for which this group is parental.
     - **Personal configuration** - list of components with personal settings, not inherited from the parental group.
   - Comparative parameters for stations:
     - **Creation time** of this station.
     - **Primary group** for this station.
     - **Personal configuration** - list of components with personal settings, not inherited from the primary group.
     - **Installed components** - list of anti-virus components installed at this station.

Chapter 6: Administration of Workstations

Anti-virus networks operated by **Dr.Web Enterprise Security Suite** provide for centralized configuring of anti-virus packages on workstations and allows:

- to set the configuration parameters of anti-virus programs,
- to schedule tasks on workstations,
- launch scanning the computer independently of schedule settings,
- to update workstations, also after an updating error, in this case the error state will be reset.

The administrator of the anti-virus network can grant a user with the permissions to change the configuration of the workstation and launch tasks, as well as restrict or prohibit such actions.

The configuration of workstations can be modified even when they are temporarily disconnected from the **Server**. These changes will be accepted by the workstations as soon as they are reconnected to the **Server**.

6.1. Management of Workstation Accounts

6.1.1. New Stations Approval Policy

Procedure of stations adding via the **Control Center** is described in the **Installation manual**, p. Creation of a New User Account.

Possibility of managing authorization of stations at **Dr.Web Server** depends on the following parameters:

1. If during the **Agent** installation, the **Manual authorization on server** flag is cleared, mode of stations access to the **Server** is defined according to settings specified at the **Server** (used by default), see below.
2. If during the **Agent** installation, the **Manual authorization on server** flag is set and **Identifier** and **Password** parameters are specified, when connecting to the **Server**, station will be authorized automatically regardless of **Server** settings (is used by default when installing the **Agent** via the *esinst* installation package - see **Installation manual**, p. Installation Files).

Setting the type of the **Agent** authorization during its installation is described in the **User Manual**.

To change the access mode of stations to Dr.Web Server:

1. Open the **Server** configuration: select the **Administration** item in the main menu, then click **Dr.Web Server configuration** in the control menu.
2. On the **General** tab, in the **Newbies registration** drop-down list select the necessary option:
   - **Approve access manually** (the mode is specified by default unless changed at the **Servers** installation),
   - **Allow access automatically**,
   - **Always deny access**.

Manual Access Approving

In the **Approve access manually** mode, new stations are placed to the **Newbies** subgroup of the **Status** group until administrator submits them.

To manage the access of unapproved stations:

1. Select the **Anti-virus Network** item in the main menu of **Dr.Web Security Control Center**. In the hierarchical list of the anti-virus network, select stations in the **Newbies** subgroup of the **Status** group.
2. To specify an access to the **Server**, in the **Unapproved stations** section of the toolbar, set the action to apply for selected stations:

   Approve selected stations and set a primary group - approve access for selected stations and set the primary group from the offered list.

   Cancel action specified to execute on connect - cancel an action under unapproved station which was specified for executing when station will connect to the **Server**.

   Reject selected stations - deny access to the **Server** for selected stations.

Access Denying

In the **Always deny access** mode, the **Server** denies access for requests from new stations. The administrator should manually create an account for new stations and set access password for them.

Automatic Access Approving

In the **Allow access automatically** mode, all stations that request an access to the **Server** will be approved automatically without requesting the administrator. The group which is set in the **Primary group** drop down list of the **Dr.Web Server configuration** section, on **General** tab, is set as a primary.

6.1.2. Removing and Restoring Stations

Removing Stations

To remove a workstation account:

1. Select the **Anti-virus network** item in the main menu, then click **General** → **Remove selected objects** in the toolbar of the opened window.
2. You will be prompt to remove the station. Click **OK**.

After a station is removed from the hierarchical list, it is added to the deleted stations table. You can restore the removed station via **Dr.Web Security Control Center**.

Restoring Stations

To restore a workstation account:

1. Select the **Anti-virus network** item in the main menu, in the opened window in the hierarchical list select deleted station or several stations you want to restore.

All deleted stations are located in the **Deleted** subgroup of the **Status** group.

2. On the toolbar, select **General** → **Restore deleted stations**.
3. The section for station restoring will be opened. You can specify the following station parameters, which will be set during restoring:
   - **Primary group** - select the primary group, in which the station will be added. By default the primary group which was set before station deletion is selected.

If you restore several stations simultaneously, the **Former primary group** is selected by default. It means that for each selected station its own primary group, in which station was resides before deletion, will be specified. If the definite group is selected, for all restoring stations the same specified group will be set.

   - In the **Membership** section, you can change the list of groups in which the station will be included. By default, the list of groups in which the station has been included before deletion is set. To include the station in a user groups, set the flags for this groups.
4. To restore the station with specified parameters, click **Restore.**

6.1.3. Merging Stations

As a result of operations with the database or reinstallation of the software on anti-virus workstations, several stations with the same name may appear on the anti-virus network list (only one of them will be correlated with the respective workstation).

To remove repeated workstation names:

1. Select all repeated names of workstation. Use the CTRL to do this.
2. In the toolbar, select **General** → **Merge stations**.
3. In the column, select the station which will be the main. All other stations will be deleted and their data will be prescribed to the selected station.
4. In the column, select the station settings of which will be set for the main station.
5. Click **Save**.

6.2. General Workstation Settings

6.2.1. Station Properties

Station Properties

To view and edit the properties of a workstation

1. Select the **Anti-virus network** item in the main menu of the **Control Center**, then select the station in the hierarchical list of the opened window.
2. Open the station properties section by one of the following ways:
   a) Click the name of the station in the hierarchical list of anti-virus network. A panel with properties of the station will be automatically opened in the right part of **Dr.Web Security Control Center**.
   b) Click **Properties** in the control menu. A window with the workstation properties will be opened.
3. Station properties pane contains the following groups of settings: **General**, **Configuration**, **Groups**, **Security**, **Location**. These settings are described below.
4. To save changes in the settings, click **Save**.

Removing Personal Settings

To remove personal settings of a workstation via Dr.Web Security Control Center:

1. Select the **Anti-virus network** item in the main menu of the **Control Center**, then select the workstation in the hierarchical list of the opened window and click **General** → **Remove personal settings** on the toolbar. A list of settings for this workstation will be opened. Personal settings will be marked with flags.
2. To remove personal settings, clear the flags and click **Delete**. Settings of the workstation inherited from the primary group will be restored.

Before editing the configuration of a workstation for **SpIDer Guard for Windows** and **Dr.Web Scanner for Windows,** familiarize yourself with recommendations on using the anti-virus for computers on Windows Server 2003 OS, Windows 2000 OS, or Windows XP OS. An article with necessary information can be found at http://support.microsoft.com/kb/822158/en. The article is meant to help you increase system performance.

Provided that your **Agent** key (`agent.key`) allows to use a spam filter for the **SpIDer Mail** component, on the **Antispam** tab you can set up the filter (on the context menu of any group or workstation, select **SpIDer Mail for workstations**).

Starting from version **5.0** anti-virus package includes **SpIDer Gate** and **Office Control** components. For using this components, they must be included in you license (**Anti-virus +Antispam**), that described in the **Agent** key file.

Spam filter, **SpIDer Gate** and **Office Control** settings are described in the manual **Dr.Web® Agent for Windows. User Manual**.

6.2.1.1. General

In the **General** section, the read-only fields are listed:

- **Station identifier** - station unique identifier;
- **Name** - station name.
- **Creation date** - the date of creation the station on the **Server**.

- **Grace period expiration** - date when the grace period of **Anti-virus** usage at the station ends.

Also you can specify the following fields:

- In the **Password** field, specify a password to authorize the station at the Server (retype this password in the **Retype password** field). If you change the password, you must repeat this action in the **Agent** connection settings at the station to permit **Agent** connection.
- In the **Description** field, add comments.

Values of fields, marked by the * sign, must be obligatory specified.

Also in this section the following links reside:

- In the **Installation file** item - the link for downloading **Agent** installer for this station.

  After creation of a new station, before the operating system of a station is set, in the section of distribution kit downloading, the links are presented separately for all OS that are supported by **Dr.Web Enterprise Security Suite**.

- In the **Configuration file** item - the link for downloading the file with settings of connection to **Dr.Web Server** for stations under Android, OS X and Linux operating systems.

6.2.1.2. Configuration

In the **Configuration** section, you can change station configuration that includes the following:

Icon	Settings	Description section
	Permissions for the workstation users	Permissions of Station Users
	Centralized schedule to run tasks on workstation	Scheduled Tasks of a Station
	License keys file for workstation	License Manager
	Restrictions on propagation of anti-virus software updates	Update Restrictions for Workstations
	Installing components list	Installing Components of the Anti-Virus Package
	Settings of anti-virus components for the station.	Management of Anti-virus Components

Dr.Web Security Control Center also provides you with option for deleting personal settings of a workstation. These settings are located on the right of the corresponding options for components configuration options. When you delete personal settings of a workstation, it inherits settings from the primary group.

When you change settings of **SpIDer Gate** and/or **Office Control**, please consider that settings of these components are interconnected, so if personal settings of one of them are removed via **Remove personal settings**, it also removes settings of second component (settings inheritance from the parent group is set).

6.2.1.3. Groups

In the **Groups** section, you can set the list of groups into which the workstation is included. The **Membership** list displays the groups which include the workstation and to which you can include it.

To manage the membership of a workstation do the following:

1. To add a station to the user group, set the flag for this group in the **Membership** list.
2. To remove a station from the user group, clear the flag for this group in the **Membership** list.

You cannot remove stations from preinstalled groups.

3. If you want to reassign the other primary group, click the icon of necessary group in the **Membership** list. The **1** sign displays on the icon.

6.2.1.4. Security

In the **Security** section, restrictions for network addresses from which **Agents** installed on the station will be able to access the **Server** are set.

To allow all connections, clear the **Use this ACL** flag. To make the list of allowed or denied addresses, set the flag.

To allow any TCP address, include it into the **TCP: Allowed** or **TCPv6: Allowed** list.

To deny any TCP address, include it into the **TCP: Denied** or **TCPv6: Denied** list.

To edit addresses in the list:

1. Specify an address in the corresponding field in the following format: *<IP address>*/[*<network prefix>*].
2. To add a new field, click in the corresponding section.
3. To delete a field, click next to the deleting address.
4. Click **Save** to apply settings.

Examples of prefix usage:

1. Prefix 24 stands for a network with a network mask: `255.255.255.0`

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`

2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16387064 addresses (256*256*256).

   Host addresses look like: `125.*.*.*`

Besides, you can delete addresses from the list and edit the addresses included into the list.

Addresses that are not included into any of the lists are allowed or denied depending on whether the **Denial priority** flag is set. If the flag is set, the **Denied** list has a higher priority than the **Allowed** list. Addresses not included in any of the lists or included into both of them are denied. Allowed only addresses that are included in the **Allowed** list and not included in the **Denied** list.

6.2.1.5. Location

In the **Location** section, you can specify additional information about the physical location of the workstation.

Also on this tab you can view the station location on a geographical map.

To view the station location on a map:

1. In the **Latitude** and **Longitude** fields, specify the station geographical coordinates in the Decimal Degrees format.
2. Click **Save** to save specified data.
3. On the **Location** tab, the OpenStreetMaps preview will be shown containing a mark according to the specified coordinates.

   If the preview cannot be loaded, the **Show on map** text displays.
4. To view the full size map, click the preview or the **Show on map** text.

6.2.2. Installed Components of the Anti-Virus Package

Components

To check which components are installed on a workstation:

1. Select the **Anti-virus network** item in **Dr.Web Security Control Center** main menu, then click the name of a group or workstation in the hierarchical list of the opened window.
2. In the opened control menu in the **General** section, select the **Installed components** item.
3. This opens a window with information on installed components: the component name; installation time; the address of the **Server** from which the component was installed; installation folder of the component on the station.

Compound of installed components list depends on:

- Components enabled in the license key file.
- Workstation OS.
- Settings specified by administrator of anti-virus network at the **Server**. Administrator is able to change the list of anti-virus package components either before **Agent** (see Anti-Virus Package Composition) installation or at any time after its installation.

It is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on servers that implement significant network functions (domain controllers, license distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** anti-virus.

Virus Bases

To view virus databases installed on a workstation:

1. Select the **Anti-virus network** item in **Dr.Web Security Control Center** main menu, then click the name of a workstation in the hierarchical list of the opened window.
2. In the opened control menu in the **Statistics** section, select the **Virus bases** item.
3. This opens a window with information on installed virus databases: the name of the file containing a particular database; virus database version; the database creation date; the total number of virus records in the database.

If the **Virus bases** item is hidden, to view the item, select **Administration** in the main menu, and then select **Dr.Web Server configuration** in the control menu of the window. On the **Statistics** tab, set **Stations status monitoring** and **Virus database monitoring** flags, then restart the **Server**.

6.2.3. Hardware and Software on Stations under Windows® OS

Dr.Web Enterprise Security Suite allows to accumulate and view information on hardware and software installed on protected stations under Windows OS.

To collect information on hardware and software of the stations:

1. Enable statistics collecting on the **Server**:
   a) Select the **Administration** item in the main menu of the **Control Center**.
   b) Select the **Dr.Web Server Configuration** item in the control menu.
   c) In the **Server** settings, open the **Statistics** tab and set the **Hardware and software** flag if it is cleared.
   d) To apply the changes, click **Save** and restart the **Server**.
2. Allow collecting statistics on stations:
   a) Select the **Anti-virus Network** item in the main menu of the **Control Center**.
   b) In the hierarchical list of anti-virus network, select a station or a group of stations for which you want to allow statistics collecting. When selecting a group of stations, please note the settings inheriting: if the stations of selected group have personal settings, when changing the group settings will not change the station settings.
   c) In the control menu, in the **Configuration** → **Windows** section, select **Dr.Web Agent**.
   d) In the **Agent** settings, on the **General** tab, set the **Collect information about stations** flag if it is cleared. If necessary, edit the **Period of collecting information about stations (min.)** parameter value.
   e) To apply the changes, click **Save**. Settings will be transmitted to the stations.

To view hardware and software of the station:

1. Select the **Anti-virus Network** item in the main menu of the **Control Center**.
2. In the hierarchical list of anti-virus network, select appropriate station.
3. In the control menu, in the **General** section, select the **Hardware and software** item.
4. In the opened window you can view the tree with the list of hardware and software, which contains the following information about the station:
   - **Application** - the list of program applications installed on the station.
   - **Hardware** - the list of hardware mounted on the station.
   - **Operating System** - information on operating system of the station.
   - **Windows Management Instrumentation** - information on Windows management instrumentation.
5. To view the detailed information on a concrete hardware or application, select the necessary object in the tree.

To compare hardware and software of several stations:

1. Select the **Anti-virus Network** item in the main menu of the **Control Center**.
2. In the hierarchical list of anti-virus network, select several stations or groups of stations. To view the comparison page, you must select two of more stations under Windows OS.
3. In the control menu, in the **General** section, select the **Comparison of hardware and software** item.
4. In the opened window, the following information is available:
   - the free with the list of hardware and software;
   - comparison table for the selected stations.
5. To display comparing data, select necessary item in the tree of hardware and software. All available values of the selected item will be displayed in the comparison tree.

6.3. Management of Workstation Configuration

6.3.1. Permissions of Station Users

To edit users permissions via Dr.Web Security Control Center for administrating the anti-virus package:

1. In the main menu, select **Anti-virus network**, then click the name of a workstation in the hierarchical list of the opened window. In the opened control menu, select **Permissions**. Permissions configuration window opens.
2. You can edit permissions on tabs that correspond to the workstation operating system. To change (allow or deny) any of permissions, set or clear the flag for this permission.
3. To edit permissions for stations under Windows, OS X, Linux and Android operating systems, use the following tabs:
   - **Components** - change permissions for components management. By default, a user is authorized to launch each component, but prohibited to edit components configuration or stop the operation of components.
   - **General** - to change permissions for **Dr.Web Agent** and its functions management:

Table 6-1. Setting stations permissions on the General tab

Permissions section flag	Flag actions	Result at the station if the flag is cleared
Stations under Windows OS		
Run in mobile mode	Set the flag to allow users at the station to switch to mobile mode and use **Dr.Web Global Update System** for updating, if there is no connection with **Dr.Web Server**.	In the **Agent** settings, in the **Main** > **Mode** section, the **Use Mobile mode when there is no connection with the server** option is not available.
Change the run mode	Set the flag to allow users at the station to change the **Agent** run mode.	In the **Agent** settings, in the **Main** > **Mode** section, the following options are not available: • **Accept updates from the server**, • **Accept jobs from the server**, • **Accumulate events**.
Change Dr.Web Agent configuration	Set the flag to allow users at the station to change **Dr.Web Agent** settings.	In the **Agent** settings, in the **Main** section, the settings of the following options are not available: • **Notifications**: all settings are not available. • **Mode**: the **Server** connection settings and the **Synchronize system time with the server time** flag are not available. • **Self-Protection**: the **Block changing of system date and time**, **Block user activity emulation** options are not available. • **Advanced**: in the **Log** section settings, the **Dr.Web Update**, **Dr.Web Services**, **Create memory dumps at scan errors** options are not available.
Change preventive protection configuration	Set the flag to allow users at the station to edit preventive protection settings.	In the **Agent** settings, in the **Protection Components** > **Preventive protection** tab, all options are not available.

Permissions section flag	Flag actions	Result at the station if the flag is cleared
Disable self-protection	Set the flag to allow users at the station to disable self-protection.	In the **Agent** settings, in the **Main** > **Self-Protection** the **Enable self-protection** option is not available.
Uninstall Dr.Web Agent	Set the flag to allow users at the station to uninstall **Dr.Web Agent**.	Disables uninstalling of the **Agent** at the station either via the installer or via standard Windows OS services. In this case, **Agent** can be uninstalled only via the **General** → **Uninstall Dr.Web Agent** option on the toolbar of **Dr.Web Security Control Center**.
Stations under OS X		
Run in mobile mode	Set the flag to allow users at the station to switch to mobile mode and use **Dr.Web Global Update System** for updating, if there is no connection with **Dr.Web Server**.	The **Updates** section in the application main window is blocked.
Stations under Linux system-based OS		
Run in mobile mode	Set the flag to allow users at the station to switch to mobile mode and use **Dr.Web Global Update System** for updating, if there is no connection with **Dr.Web Server**.	For the console mode of the application: the `drweb-ctl update` command for updating the virus databases from the **GUS** is not available.
Stations under Android OS		
Run in mobile mode	Set the flag to allow users of mobile devices to switch to mobile mode and use **Dr.Web Global Update System** for updating, if there is no connection with **Dr.Web Server**.	The **Updates** section on the application main screen is blocked.

After disabling an option that changes **Agent** settings, the value which has been set at the last time before disabling, will be used.

Actions for the corresponding menu options are described at the **Dr.Web® for Windows. User manual** documentation.

4. To use the same settings for another object, click **Propagate these settings to another object**.
5. To export settings to a file, click **Export settings from this section to the file**.
6. To import settings from a file, click **Import settings to this section from the file**.
7. To save permissions changes, click **Save**.

If you have edited a workstation, when it was not connected to the **Server**, the new settings will be accepted, once the **Agent** has reconnected to the **Server**.

6.3.2. Scheduled Tasks of a Station

Dr.Web Enterprise Security Suite provides the *centralized task schedule* which is set by the anti-virus network administrator and complies with all the rules of configuration inheritance.

Task schedule – a list of actions performed automatically at a preset time on workstations. Schedules are mostly used to scan stations for viruses at a time most convenient for users, without having to launch the Scanner manually. Besides **Dr.Web Agent** allows to perform certain other types of tasks as described below.

To edit centralized schedule of regular tasks execution for certain stations and groups, use **Dr.Web Security Control Center**.

To edit centralized schedule, perform the following actions:

1. Select the **Anti-virus network** item in the main menu of the **Control Center**, in the hierarchical list of the opened window, select a group or workstation. In the opened control menu, select **Task Scheduler**. The list with the tasks of the station will be opened.

   By default for stations operated under Windows OS, schedule contains the **Daily scan** task - daily station scan (disabled).

2. To manage schedule, use the corresponding elements from the toolbar:

   a) General elements on the toolbar are used to create new tasks and generally manage schedule section. These tools always available on the toolbar.

   Create task - add a new task. This action is described in details below, in the Task Editor section.

   Propagate these settings to another object - copy sheduled tasks into other objects - stations and groups. For details, see Propagation of Settings to Other Groups/Stations.

   Export settings from this section to the file - export schedule to the file of special format.

   Import settings to this section from the file - import schedule from the file of special format.

   b) To manage existing tasks, set the flags for the necessary tasks or in the table header to select all task from the list. The elements on the toolbar to manage selected tasks become available.

Table 6-2. Toolbar elements for managing selected tasks

Option		Action
Status	**Enable execution**	Activate execution of selected tasks according to their schedule, if they were disabled.
	Disable execution	Disable execution of selected tasks. Tasks remain on the list but will not be executed.
The same action you can perform from the task editor on the **General** tab by setting the **Enable execution** flag.		
Severity	**Make critical**	Perform extra launch of the task at next **Dr.Web Agent** launch, if scheduled execution of this task has been omitted.
	Make not critical	Execute the task only at scheduled time regardless of whether a task launch has been omitted or not.
The same action you can perform from the task editor on the **General** tab by setting the **Critical task** flag.		
Duplicate settings		Duplicate tasks that are selected in the list of current schedule. When you run the **Duplicate settings** option, new tasks are created with settings similarly to the selected tasks.

Option	Action
Schedule repeatedly	For tasks which executed once: execute task one more time according to the specified time settings (changing execution multiplicity of the task is described below, in the Task Editor section).
Remove these settings	Remove selected task from the schedule.

3. To change task parameters, select it in the tasks list. The **Task editor** window described below opens.
4. After editing the schedule, click **Save** to accept changes.

If, when edited, the schedule is empty (without any tasks), **Dr.Web Security Control Center** will offer you to use either the schedule inherited from groups, or the empty schedule. Use empty schedule to override the schedule inherited from the groups.

Task Editor

In the **Task Editor** you can specify settings to:

1. Create a new task.

   For this click **Create task** on the toolbar.

2. Edit existing task.

   For this click the name of one of the tasks in the tasks list.

The window for editing a task opens. Settings for editing of existing task are similar to the settings of creating a new task.

Values of fields, marked with the * sign, must be obligatory specified.

To edit task settings:

1. On the **General** tab you can setup the following parameters:
   - In the **Name** field, specify the name of the task displayed in the schedule list.
   - To enable the task execution, set the **Enable execution** flag. If the flag is cleared, the task remains on the list but will not be executed.

   The same action you can perform from the main window of the schedule via the **Status** option on the toolbar.

   - The **Critical task** flag instructs to perform extra launch of the task at next **Dr.Web Agent** launch, if scheduled execution of this task has been omitted (**Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after **Dr.Web Agent** has been launched.

   The same action you can perform from the main window of the schedule via the **Severity** option on the toolbar.

   If several scan tasks must be implemented, only one task will be executed - the first one in the queue.

For example, if **Daily scan** is enabled and critical scan via the **Agent Scanner** is omitted, only **Daily scan** will be executed and omitted critical task will not be done.

2. On the **Action** tab, in the **Action** drop-down list, select the type of the task and specify task parameters which are needed to perform the task.

Table 6-3. Tasks types and parameters

Task type	Parameters and description
Write to log file	**String** - the text of the message to be added to the log file.
Run program	Specify the following settings: ◆ The **Path** field – full name (with the path) of the executable file to be launched. ◆ The **Arguments** field – line parameters for the program to be run. ◆ Set the **Execute synchronously** flag to wait while task finishes before executing other tasks with **Run program** type. If the **Execute synchronously** flag is cleared, the **Agent** logging only the start of the program. If the **Execute synchronously** flag is set, the **Agent** logging the start of the program, the returned code and the time of the program shutdown.
Dr.Web Scanner. Complete scan **Dr.Web Scanner. Custom scan** **Dr.Web Scanner. Express scan**	Parameters of scanning setup are described in the Configuring Scanner Settings.

Remote launch of the **Scanner** is available only on stations under Windows OS, UNIX system-based OS and OS X.

3. On the **Time** tab:
   ◆ In the **Period** drop-down list set the launch mode of the task and setup the time according to the specified periodicity.

Table 6-4. Parameters of different launch modes

Launch type	Description
Daily	Specify the hour and the minute for the task to be launched at the time specified.
Every N minutes	The **N** value should be specified to set the time interval for the execution of the task. At **N** equal 60 or more, the task will be run every **N** minutes. At **N** less than 60, the task will be run every minute of the hour multiple of **N**.
Hourly	Specify a number from 0 to 59 to set the minute of every hour the task will be run.
Monthly	Specify the day of the month, the hour and the minute for the task to be launched at the time specified.
N minutes after initial task	In the **Initial task** drop-down list, select the task relatively to which the time of current task execution is set. In the **Minute** field, specify or select from the offered list the number of minutes that should pass after the execution of initial task to start execution of edited task.
Start up	The task will be launched at **Agent** start up. No additional parameters required to run the task.
Weekly	Select a day of the week, specify the hour and the minute, for the task to be launched at the time specified.

- Set the **Disable after the first execution** flag to execute the task only once at specified time. If the flag is cleared, the task will be executed multiple times according to the specified periodicity.

To repeat the launch of task already ones executed, use the **Schedule repeatedly** on the toolbar of the schedule section.

4. When all parameters for the task are specified, click **Save** to accept changes of edited parameters, if you editing existing task, or to create a new task with specified parameters if you created a new task.

6.3.3. Installing Components of the Anti-Virus Package

To change the installing components list of the anti-virus package:

1. Open the list of components, select the **Anti-virus network** item in the main menu, then select the station and click the **Installing Components** item in the control menu.
2. Select an option for necessary components in the drop-down list:
   - **Must be installed** - means that a component *must* be present on the workstation. When a new workstation is created, the component is installed with the anti-virus package. If the **Must be installed** option is specified for an existing workstation, the component will be added to the available anti-virus package.
   - **May be installed** - means that the component can potentially be installed. The user decides whether the component is required.
   - **Cannot be installed** - means that installing the component is not allowed. When a new workstation is created, the component will not be installed with the anti-virus package. If the **Cannot be installed** option is specified for an existing workstation, the component will be removed from the anti-virus package.

   Table 6-5 shows whether the component will be installed on the workstation (+) according to the parameters specified by the user and the settings defined by the **Server** administrator.

Table 6-5.

User parameters	Specified on the Server		
	Must	May	Cannot
Install	+	+	
Do not install	+		

3. Click **Save** to save the settings and the set of anti-virus package components on the workstation.

The **Dr.Web Anti-spam** component cannot be installed, if at least one of the listed products is not installed:

- **SpIDer Mail**,
- **Dr.Web for Microsoft Outlook**.

6.4. Management of Anti-virus Components

To view and edit the configuration of the anti-virus components on the workstation:

1. Select the **Anti-virus network** item in the main menu of the **Control Center**.
2. Click name of the station or group in the hierarchical list of the opened window.
3. In the opened control menu, in the **Configuration** section, in the subsection that corresponds the operating system of selected stations, select the necessary component.
4. A window with the component settings will be opened.

The list of anti-virus component settings and setup recommendations are listed in the **User Manual** for corresponding operating system.

But some settings of the components in the **Control Center** and on workstations may differ by the level of detail.

This Manual contains **Dr.Web Agent for Windows** settings which are presented as extended settings of the **Agent**, provided to a user on a station, and also anti-virus components settings which are not provided on protected stations.

When configuring anti-virus components for station under Windows OS, please note the following logging points:

- On the **Control Center**, logging settings are specified separately for each component in the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.
- If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This led to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).
  Debug logging mode decrease performance of **Anti-virus** and operating system of a station. It is recommended to use this mode only when errors occur in component operation or by request of technical support service. It is not recommended to enable logging debug mode for a long time.

Dr.Web Security Control Center interface is somewhat different from the interface of the anti-virus components:

- to manage separate parameters, use the options located on the right from corresponding settings:
  - **Reset to initial value** - restore the value that parameter had before editing.
  - **Reset to default value** - set the default value for a parameter.
- to manage set of parameters, use the options located in the toolbar:

  Reset all parameters to initial values - restore the values that all parameters in this section had before current editing (last saved values).

  Reset all parameters to default values - restore default values of all parameters in this section.

  Propagate these settings to another object - copy settings from this section to settings of other station, group or several groups and workstations.

  Set inheritance of settings from primary group - remove personal settings of a station and set inheritance of settings in this section from a primary group.

  Copy settings from primary group and set them as a personal - copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered as a personal.

  Export settings from this section to the file - save all settings from this section to a file of a special format.

Import settings to this section from the file - replace all settings in this section with settings from the file of a special format.

5. If any changes in the settings are made via **Dr.Web Security Control Center**, click **Save** to accept the changes. The settings will be passed to the stations. If the stations were offline when changes are made, the settings will be passed when stations connect to the **Server**.

6.4.1. Components

Depending on the operating system of the station, the following anti-virus components are provided:

Stations under Windows® OS

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** including rootkits check is supported.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

SpIDer Mail

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is is also available (if the license permits this function).

SpIDer Gate

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office control

Controls access to network and local resources, in particular, limits access to web sites. Allows to control the integrity of important files from the accidental change or virus infecting and limit the access to unwanted information for employees.

Firewall

Protects computers from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Self-protection

Protects files and folders of **Dr.Web Enterprise Security Suite** from unauthorized or accidental removal and modification by user or malicious software. If self-protection is enabled, access to files and folders of **Dr.Web Enterprise Security Suite** is granted to **Dr.Web** processes only.

Preventive protection (settings are provided into Dr.Web Agent settings)

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocking them in case of detection of viral activity.

Stations under UNIX® system-based OS

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

SpIDer Gate

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Other components settings of which are given in the **Control Center** for stations under UNIX system-based OS, are additional and serve for internal configuration of anti-virus software operation.

Stations under OS X®

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Mobile devices under Android OS

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a mobile device on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

SpIDer Guard

The constant file system protection in the real-time mode. The check of all files as they are saved in the memory of the device.

Calls and SMS Filter

Filtering the incoming phone calls and SMS allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detect the device location or lock its functions in case it has been lost or stolen.

Cloud Checker

URL filter allows to protect user of the mobile device from unsolicited Internet sites.

Firewall (settings are available on a mobile device only)

Protects the mobile device from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Security Auditor (settings are available on a mobile device only)

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

Application filter

Blocks the launch on mobile device those applications that are not included into the list of allowed by administrator.

Servers under Novell® NetWare® OS

Dr.Web Scanner

Scans a computer on user demand and according to the schedule.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

6.4.2. Managing Dr.Web Agent for Windows®

To view and edit the configuration of Dr.Web Agent on the station under Windows OS:

1. Select the **Anti-virus network** item in the main menu of the **Control Center**.
2. Click the name of the station or group in the hierarchical list of the opened window.
3. Click the **Configuration** > **Windows** > **Dr.Web Agent** item in the control menu.
4. A window with **Agent** settings will be opened.

Any changes incompatible with the **Server** settings (for example, changes of the encryption and compression modes) will result in disconnection of the **Agent** from the **Server**.

5. If any changes in the **Agent** settings are made via **Dr.Web Security Control Center**, click **Save** to accept the changes.

6.4.2.1. General

On the **General** tab, you can set the following parameters of the **Agent**:

- In the **Task Scheduler startup delay (min.)** filed, specify the time interval between start of the OS and execution of the startup scan task, if it was scheduled for the **Agent**. The 1 minute delay is by default. Set the 0 value to perform the scan task without any delay, i.e. immediately after the start of OS.
- In the **Period of statistics sending (min.)** field, specify the value of the time interval in minutes for the **Agent** to send to the **Server** all statistics data, collected by the **SpIDer Guard**, **SpIDer Mail** and **SpIDer Gate** components at the station. Specify the 0 value to desable statistics sending.
- In the **Language** drop-down list, specify the language for the **Agent** and **Dr.Web Anti-virus** components interface at the station or group of stations.
- Set the **Enable Microsoft Network Access Protection** flag to enable station state monitoring using *Microsoft® Network Access Protection (NAT)* technology. This enables the *System Health Agent* (SHA) which is automatically installed in a workstation with **Dr.Web Agent** software. (for more details see p. NAP Validator).
- Set the **Allow quarantine remote control** flag to enable remote control of workstations **Quarantine** from the **Server**.

The **Allow quarantine remote control** option is available if in the **Administration** → **Dr.Web Server configuration** → **Statistics** tab, the **Quarantine state** flag is set.

- Set the **Collect information about stations** flag to enable collecting information about software and hardware at the stations. When the flag is set, in the **Period of collecting information about stations (min.)** drop-down list select period in minutes of sending actual information on hardware and software from station by **Agent** to the **Server**.
- Set the **Synchronize time** flag to enable system time synchronization on the **Agent** computer with the time on the computer with **Dr.Web Server** installed.
- Set the **Block changing of system date and time** flag to prevent manual and automatic change of system time settings except time synchronization with **Dr.Web Server** (is set by the **Synchronize time** flag).
- Set the **Block user activity emulation** flag to prevent any changes in **Dr.Web** operation, except those made manually by user.

- Set the **Connect to cloud services** flag to connect the station to **Doctor Web** cloud services. This allows anti-virus components of the station to check the data on threats according to the information received in real-time mode from **Doctor Web** servers. In turn, data about **Dr.Web** components operation on the station will be automatically sent to **Doctor Web** servers.

6.4.2.2. Network

On the **Network** tab, you can specify parameters determining interaction with the **Server**:

- In the **Public key** field specify the public encryption key of **Dr.Web Server** (`drwcsd.pub`) which is stored at the station. To select the key file, click .

  Several public keys can be stored at the station at the same time, e.g., during the process of encryption keys replacement or during moving from one **Server** to another. Note that keys must be unique, i.e. you cannot specify two similar public keys.

  To add one more public key, click and select the key file.

  To remove existing key from the station, click .

  If the **Allow operating without public key** flag is cleared, you cannot remove the last public key.

- Set the **Allow operating without public key** flag to allow connecting **Agents**, if they do not have public encryption key (`drwcsd.pub`) or the file has incorrect structure.
- Set the **Allow operating with invalid public key** flag to allow connecting **Agents**, if they have incorrect public encryption key (`drwcsd.pub`).
- In the **Server** field, you can specify the address of **Dr.Web Server**. You may leave this field blank. Then the **Agent** will use as the address of **Dr.Web Server** the value of the parameter that is set on the user's local computer (the address of the **Server** from which the installation performed).

  Either one **Server** address or several different **Servers** addresses can be set. To add one more **Server**, click and specify an address in the added field. Format of **Server** network addresses is described in the **Appendices** document, in the Appendix E. The Specification of Network Addresses section.

  Server address example:

  ```
  tcp/10.4.0.18:2193
  tcp/10.4.0.19
  10.4.0.20
  ```

  If the **Server** parameter is set incorrectly, the **Agents** will disconnect from the **Server** and will not be able to reconnect. In this case you will have to set the **Server** address on the stations directly.

- In the **Search retries number** field, set the parameter determining the number of attempts to find **Dr.Web Server** via the connection using the Mulicasting mode.
- In the **Search timeout (sec.)** field, set the interval between attempts to find **Dr.Web Server** in seconds via the connection using the Mulicasting mode.
- The **Compression mode** and **Encryption mode** fields determine the compression and encryption settings of network traffic correspondingly (also see p. Traffic Encryption and Compression).
- In the **Network listening parameters** field, specify the UDP port for **Dr.Web Security Control Center** to search for working **Dr.Web Agents** in a network. To disable ports listening, enter **NONE**.

This parameter should be specified in the network addresses format described in the **Appendixes** document, in the Appendix E. The Specification of Network Addresses section.

By default, the **udp/:2193** is used, which means "all interfaces, port 2193".

6.4.2.3. Mobility

On the **Mobility** tab, you can specify parameters of *Mobile Mode* of the **Agent**:

Information on **Agents** operation in the Mobile mode is given in the Updating Mobile Dr.Web Agents section.

- In the **Update period (sec.)** field, specify the time interval between anti-virus software updates, in seconds.
- Set the **Use proxy server** flag to use an HTTP proxy server to receive updates from the Internet. This will make the fields to set a proxy server available.

6.4.2.4. Log

On the **Log** tab, you can specify parameters of **Agent** and some **Dr.Web** anti-virus components logging:

- The **Agent log verbosity level** parameter determines the level of detail of **Agent** logging.
- The **Engine log verbosity level** parameter determines the level of detail of Scanning Engine logging.
- The **Update log verbosity level** parameter determines the level of detail of **Dr.Web** updating module logging.
- Set the **Create memory dumps at scan errors**, to create memory dumps in cases of scan errors occur. It is recommended to enable this setting for **Dr.Web** operation errors analysis.

6.4.2.5. Interface

On the **Interface** tab, you can specify the parameters of the **Agent** interface:

- Set the **Show icon in taskbar** flag to display **Agent** icon in the taskbar. If icon is disabled, user cannot view and edit settings of **Agent** and anti-virus package.
- Set the **Show reboot request** flag to display a request on station reboot. If the flag is cleared, request is not displayed at the station and automatic reboot is not performed. Statistics of a station received by the **Control Center**, contains notification on the need of station reboot. Information on a state that requiring reboot is displayed in the State table. Administrator is able to reboot a station from the **Control Center** if it is needed (see the Anti-Virus Network section).

To select the type of events that a user is to be notified of, set the respective flag:

- **Critical notifications** - receive only critical notifications. Such notifications include periodical reminders about:
  - updating errors of the anti-virus software or some of the components;
  - the necessity to restart a computer after updating.

  The notification shows, if the user has administrator rights.
- **Threats notifications** - receive only notifications about viruses. This type of notification includes messages about virus (viruses) detection by one of the anti-virus software components.
- **Major notifications** - receive only important notifications. Such notifications include messages about:
  - the launching errors of the anti-virus software or some of the components;

- the updating errors of the anti-virus software or some of the components, is displayed right after error of update procedure;
- the necessity to restart a computer after updating, is displayed right after update procedure;
- necessity of message with reboot requirement to finish components installation.

◆ **Minor notifications** - receive only minor notifications. Such notifications include messages about

- the starting of remote scanning;
- the stoping of remote scanning;
- the beginning of updating of the anti-virus software or some of the components;
- the end of successful updating of the anti-virus software or some of the components.

If you want messages of all groups to be sent, set all the four flags. Ohterwise only message of the specified groups will be displayed.

Users can configure all notifications except **Critical notifications**, which are configured by administrators only.

Events receiving can be set via the **Control Center** only till the first changing of these settings at the user side. After setting personal settings at the user side, events receiving can be configured via the **Agent** context menu only.

In the **Additional** subsection, you can specify the following settings:

◆ Set the **Do not show notifications in full-screen mode** flag to disable popup notifications if any program is running in full-screen mode.

◆ Set the **Display Firewall notifications on separate desktop in full-screen mode** flag to display **Dr.Web Firewall** notifications on separate desktop, i.e. on top of running full-screen application. It is recommended to enable this option to avoid blocking of network connections which are used by this full screen mode application without possibility to enable them in the time of **Dr.Web Firewall** request receipt.

6.4.2.6. Preventive Protection

On the **Preventive Protection** tab in the **Level of suspicious activity blocking** section, you can configure **Dr.Web** reaction on such actions of other programs that may cause workstation infection. You can also protect user data from unwanted changes.

Select one of protection levels that anti-virus provides:

◆ **Paranoid** - maximal protection level when you need total control of access to critical Windows OS objects.

Using this mode may lead to compatibility problems with legitimate software that uses the protected registry branches.

◆ **Medium** - protection level at high risk of computer getting infected. In this mode, the access to the critical objects that can be potentially used by malicious software is additionally blocked.

◆ **Minimum** - protection level that disables automatic changes of system objects, modification of which explicitly signifies a malicious attempt to damage the operating system.

◆ **Custom** - protection level that is set by a user (**Server** administrator) and based on settings specified in the table below.

To specify custom settings of preventive protection level, set the flags in the table of this section to the one of the following position:

- **Allow** - always allow actions with this object or from this object.

- **Ask** - prompt the dialog box for setting necessary action by the user for the specific object.
- **Block** - always deny actions with this object or from this object.

If you change table settings when one of preinstalled levels in the **Level of suspicious activity blocking** section is set, it automatically changes to **Custom**.

Preventive protection settings allow to monitor the following objects:

- **Integrity of running applications** - detect processes that inject their code into running applications that may compromise computer security. Processes that are added to the exclusion list of **SpIDer Guard** component are not monitored.
- **Integrity of users files** - detect processes that modify user files with the known algorithm which indicates that the process may compromise computer security. Processes that are added to the exclusion list of **SpIDer Guard** component are not monitored. To protect your data from unauthorized modifications, it is recommended to set the creation of protected copies for important files.
- **HOSTS file** - the operating system uses this file for simplifying access to the Internet. Changes to this file may indicate virus infection or other malicious program.
- **Low level disk access** - block applications from writing on disks by sectors avoiding the file system.
- **Drivers loading** - block applications from loading new or unknown drivers.

Other options control access to critical Windows OS objects and allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).

Table 6-5. Protected registry branches

Parameter	Registry branch
Image File Execution Options	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
User Drivers	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Winlogon parameters	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Winlogon notifiers	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Windows shell autorun	Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Executable files associations	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys)
Software Restriction Policies	Software\Policies\Microsoft\Windows\Safer
Internet Explorer extensions (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Program autorun	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Policy autorun	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Safe mode configuration	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Session Manager parameters	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows

Parameter	Registry branch
System services	System\CurrentControlXXX\Services

If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), disable the corresponding options in this group.

6.4.3. SpIDer Mail for Windows® Configuration. Application Filter

Application filter allows to configure manual interception of mail traffic. In this mode, **SpIDer Mail** serves as a proxy between mail clients and mail servers and intercepts only those connections that are explicitly defined in the settings. To use this mode, you need also to configure mail clients on stations.

The list of intercepted addresses includes records each one of which establishes a correspondence between settings of **SpIDer Mail** and a mail server.

By default, the interception list is empty. You can add necessary records.

Configuring Mail Interception

1. Make a list of all mail servers whose connections you want to intercept and assign port numbers for these servers in arbitrary order. At this, use only unused non-system ports. The assigned numbers are called *SpIDer Mail ports*.

SpIDer Mail supports POP3, SMTP, IMAP4, and NNTP mail servers.

2. Select the **Anti-virus network** item in the main menu of the **Control Center**.
3. Click the name of the station or group in the hierarchical list of the opened window.
4. Click the **Configuration** > **Windows** > **SpIDer Mail** item in the opened control menu. Open the **Application filter** tab.
5. In the **SpIDer Mail connections settings** section, specify the following parameters:
   - **SpIDer Mail port** – *SpIDer Mail port* that you assigned for the mail server at step 1;
   - **Server** – the domain name or IP address of the mail server;
   - **Port** – the port number that the mail server uses.
6. If necessary, repeat the step 5 for other servers. To add one more mail server to the list, click .
7. To stop intercepting connections to a certain mail server, click next to the item of the list that corresponds to this server.
8. In the **Excluded applications** list, you can specify the list of applications whose mail traffic will not be intercepted and checked by **SpIDer Mail**:
   a) To exclude the application from the check, specify the path to the executable file of this application.
   b) Only one excluded application is specified in each field. To add one more element to the list, click .
   c) To remove an application from the exclusions list, click next to the item of the list that corresponds to this application.
9. After you configure all necessary settings, click **Save** to apply the changes on the station.

The **Application filter** of the **SpIDer Mail** component can be configured on **Dr.Web Server** only. Corresponding settings are not provided at the station.

10. Configure the mail client at the station to support the manual interception mode by the **SpIDer Mail** component.

Configuring Mail Clients

If the **SpIDer Mail** configured to manual intercept connections with mail servers, change the settings of a mail client on the station as the following:

1. Set the addresses of the incoming and outgoing mail servers as `localhost`.
2. Set the mail server port to the *SpIDer Mail port* number that you assigned to the corresponding mail server.

Usually, you need to specify the following in the mail server settings:

`localhost`:<*SpIDer_Mail_port*>

where <*SpIDer_Mail_port*> is the number that you assigned to the mail server.

For example

If you assigned the `7000` *SpIDer Mail port* to a mail server that uses the `110` port and the `pop.mail.ru` address, then set mail client to connect to `localhost` via the `7000` port.

6.5. Anti-Virus Scanning of Stations

Users can scan their workstations themselves using **Dr.Web Scanner for Windows**. A **Scanner** shortcut is created on the desktop during the installation of the anti-virus package. The Scanner can be launched and operate successfully even in case of **Agent** malfunction or running Windows OS in the safe mode.

Via the Control Center you can:

- View the list of all anti-virus components running at present.
- Terminate running anti-virus components of a certain type.
- Initiate anti-virus scanning and specify its parameters.

6.5.1. Viewing and Terminating Running Components

To view the list of running components and terminate some of them manually:

1. In the main menu, select **Anti-virus network**, then click the name of a workstation or group in the hierarchical list of the opened window. In the control menu, select **Running components**.

   Lists of components active at present such as launched via the Control Center manually by administrator or scheduled and launched by a users at the station, will be opened.

2. If you want to interrupt any of components, set the flag next to this component and click **Interrupt** on the toolbar. Execution of a task will be terminated, and the tasks will be removed from the list.

When you use this option, running scans will be terminated, **Scanner** stopped and running monitors paused.

Attention! You cannot launch **SpIDer Guard**, **SpIDer Mail** and **SpIDer Gate** monitors via **Dr.Web Security Control Center**.

6.5.2. Terminating Running Components by Type

When you use this option, running scans will be terminated, **Scanner** stopped and running monitors paused.

Attention! You cannot launch **SpIDer Guard**, **SpIDer Mail** and **SpIDer Gate** monitors via **Dr.Web Security Control Center**.

To interrupt all running components of a certain type

1. Select **Anti-virus network** in the main menu of the **Control Center**, then in the hierarchical list of the opened window select necessary group or separate workstations.
2. In the toolbar of anti-virus network, click **Components management**. In the drop-down list select **Interrupt running components**.
3. In the opened panel, set the flags against components types which you want to interrupt immediately:
   - **Interrupt scheduled Dr.Web Agent Scanner** - to stop active scan by **Dr.Web Agent Scanner** which was launched manually by administrator via the **Control Center**.
   - **Interrupt Dr.Web Agent Scanner started by administrator** - to stop active scan by **Dr.Web Agent Scanner** which was launched according to centralized schedule.
   - **Interrupt Dr.Web Scanner started by user** - to stop active scan by **Dr.Web Scanner** which was launched by a user at the station.
   - **Interrupt SpIDer Guard, SpIDer Mail, SpIDer Gate, Office Control, Firewall and Self-protection** - to pause **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate**, **Firewall** and **Self-protection** components.

   To select all types of interrupting components, set the flag against the header of the **Interrupt running components** panel.
4. Click **Interrupt**.

6.5.3. Launching Scan on Station

To launch a scan task:

1. In the main menu of **Dr.Web Security Control Center**, select **Anti-virus network**.
2. Click the name of a station or group in the hierarchical list of the opened window.
3. In the toolbar, click **Scan**. In the opened list at the toolbar, select one of the following scan modes:

   Dr.Web Scanner. Express scan. In this mode the following objects will be scanned:

   - main memory (RAM),
   - boot sectors of all disks,
   - autorun objects,
   - root directory of the boot sector,
   - root directory of the Windows OS installation disk,

- system directory of the Windows OS,
- `My documents` folder,
- temporary directory of the system,
- temporary directory of the user.

Dr.Web Scanner. Complete scan. In this mode complete scan of hard disks and removable disks (including the boot sectors) is performed.

Dr.Web Scanner. Custom scan. In this mode you may select any files and folders to scan. and Specify extended parameters of the check.

You can launch the **Scanner** only if you select active stations running under OS that supports the **Scanner** launch: Windows OS, UNIX system-based OS and OS X.

4. After you select scan type, the **Scanner** settings window will be opened. Change scanning parameters if necessary (see the Configuring Scanner Settings section).
5. Click **Scan for viruses** to launch the scan process on selected workstations.

Station scanning via **Dr.Web Agent Scanner** that is launched remotely, is performed in the background mode without displaying any notifications for station user.

6.5.4. Configuring Scanner Settings

Via the Control Center, you can specify the following anti-virus check parameters:

- **Dr.Web Scanner** settings. This **Scanner** is launched by users on stations and cannot be remotely launched from the **Control Center**. But administrator is can centralized change its settings which will be transmitted and saved on stations.
- **Dr.Web Agent Scanner** settings. This **Scanner** is remotely launched from the **Control Center** and performs station check similarly to **Dr.Web Scanner**. **Dr.Web Agent Scanner** settings are presented as extended settings of **Dr.Web Scanner** and specified during the launch of stations anti-virus check.

Dr.Web Scanner Parameters Setup

1. In the main menu of **Dr.Web Security Control Center**, select **Anti-virus network**.
2. Click the name of a station or group in the hierarchical list of the opened window.
3. In the opened control menu in the **Configuration** section, select in the necessary operating system subsection the **Scanner** item. The **Scanner** settings window opens.
4. Specify necessary scan parameters. Description of **Dr.Web Scanner** parameters is given in the **User Manual** for corresponding operating system.
5. Click **Save**. Settings will be saved in the **Control Center** and transmitted to the corresponding stations.

Dr.Web Agent Scanner Parameters Setup

Dr.Web Agent Scanner parameters are specified during the launch of stations anti-virus check as described in the Launching Scan on Station section.

The list of **Scanner** settings sections which are available (+) or not available (–) depends on the mode of station scan launch and presented in the table below.

Table 6-6. The list of Scanner settings sections depending on the scan launch

Scan launch mode	Settings sections			
	General	Actions	Limitations	Exclusions
Dr.Web Scanner. Custom scan	+	+	+	+
Dr.Web Scanner. Express scan	–	+	+	–
Dr.Web Scanner. Complete scan	–	+	+	–

Depending on the operating system of the stations on which the remote scan is launched, only those part of **Scanner** settings is available, which is supported by station system.

Settings that are not supported in check of stations under UNIX system-based and MAS OS X are marked with the [] sign.

6.5.4.1. General

Settings that are not supported in check of stations under UNIX system-based and MAS OS X are marked with the [] sign.

In the **General** section, you can configure the following settings of anti-virus check:

- Set the **Use heuristic analysis** flag so **Scanner** will check for unknown viruses via the heuristic analyzer. In this mode the **Scanner** may give false positives though.
- The **Scan boot sectors** flag so **Scanner** will check boot sectors of the drives. Both boot sectors of logical drives and main boot sectors of physical drives are scanned.
- The **Scan programs that run on startup**[] flag to scan files that automatically launched at operating system startup.
- Set the **Follow symbolic links** flag to follow symbolic links during scan.
- See the **Scan running programs and modules**[] flag to scan processes that are run in the RAM.
- Set the **Scan for rootkits**[] flag to enable scanning for malware that hides its presence in the system.
- Set the **Interrupt scanning when switching to battery mode**[] flag to interrupt scanning when switching computer of a user to battery mode.
- The **Scan priority** drop-down list defines priority of the check process relatively computing resources of operating system.
- Set the **Load level of computer resources**[] flag to limit the use of computer resources when scanning, set the flag and select from the drop-down list the maximum allowed load of resources by **Scanner**. In absence of other tasks, computer resources are used in maximum.

The **Load level of computer resources** option has no effect on the actual resources load when launching the scan on a single-processor system with one core.

- The **Actions after scan** drop-down list instructs to perform specified action automatically when the check is completed:
  - **do nothing** - no actions perform on user computer after the check is completed.
  - **shutdown station**[] - shutdown the user computer after the check is complete. Before shutdown the computer, the **Scanner** applies specified actions to detected threats.

- **reboot station** - restart the user computer after the check is complete. Before restart the computer, the **Scanner** applies specified actions to detected threats.
- **suspend station**.
- **hibernate station**.

- Set the **Disable network while scanning** flag to disable network and Internet connections during scanning process.
- Set the **Scan fixed volumes** flag to scan fixed hard drives (hard disk drives, etc.).
- Set the **Scan removable media** flag to scan all removable data storages such as floppy or CD/DVD disks, flash drives etc.
- In the **Paths selected for scan** field, specify the list of checked paths (how to specify paths is described below).
  - To add a new string to the list, click and specify required path to the opened string.
  - To remove an item from the list, click next to the corresponding string.

  If you set the **Paths selected for scan** flag, only specified paths will be scanned. If the flag is cleared, all disks will be checked.

6.5.4.2. Actions

Settings that are not supported in check of stations under UNIX system-based and MAS OS X are marked with the [-] sign.

On the **Actions** tab, you can configure reactions of **Scanner** on detection of infected or suspicious files, malware and infected archives.

Dr.Web Agent Scanner automatically applies actions that are specified for detected virus threats.

The following actions for detected virus threats are provided:

- **Cure** - restore the original state of an object before infection. If the object is incurable, or the attempt of curing fails, the action set for incurable viruses is applied.

  Available for known viruses only except Trojan programs that are deleted on detection, and infected files within complex objects (archives, mail boxes or file containers).

- **Delete** - delete infected object.
- **Move to quarantine** - move the object to the special **Quarantine** at the station.
- **Report** - send a notification to the **Control Center** about the detection of a virus (see the Setting Alerts section on how to configure alerts).
- **Ignore** - skip the object without performing any action and do not send notification in the scan statistic.

Table 6-7. Reactions of Scanner to various virus events

Object	Action				
	Cure	Delete	Move to quarantine	Report	Ignore
Infected	+/*	+	+		
Suspicious		+	+/*		+
Incurable		+	+/*		
Containers		+	+/*		

Object	Action				
	Cure	Delete	Move to quarantine	Report	Ignore
Archives		+	+/*		
E-mail files			+/*		+
Boot sectors	+/*			+	
Adware		+	+/*		+
Dialers		+	+/*		+
Jokes		+	+/*		+
Riskware		+	+/*		+
Hacktools		+	+/*		+

Conventions

+	action is enabled for this type of objects
+/*	action is set as default for this type of object

To set actions on virus threats detection, use the following options:

- The **Infected files** drop-down list specifies the **Scanner** reaction to the detection of a file infected with a known virus.
- The **Suspicious files** drop-down list specifies the **Scanner** reaction to the detection of a file presumably infected with a virus (upon a reaction of the heuristic analyzer).

If scanning includes the OS installation folder, it is recommended to select the **Report** action for suspicious files.

- The **Incurable files** drop-down list specifies the **Scanner** reaction to the detection of a file infected with a known incurable virus and in case if attempt to cure a file is failed.
- The **Infected containers** drop-down list specifies the **Scanner** reaction to the detection of an infected or suspicious file in a file container.
- The **Infected archives** drop-down list specifies the **Scanner** reaction to the detection of an infected or suspicious file in a file archive.
- The **Infected archives** drop-down list specifies the **Scanner** reaction to the detection of an infected or suspicious file in e-mail format.

If viruses or suspicious program code is detected within complex objects (archives, e-mail attachments or file containers), an actions selected for this type of a complex object is performed to a whole object, not just to the infected part. By default informing the user on the threat is performed.

- The **Infected boot sectors** drop-down list specifies the **Scanner** reaction to the detection of an viruses or suspicious program code in the boot sectors area.
- In the following drop-down list, set the **Scanner** reaction to the detection of corresponding type of unsolicited software:
  - **Adware**;
  - **Dialers**;
  - **Jokes**;
  - **Riskware**;
  - **Hacktools**.

If you select **Ignore**, no action is performed: no notifications are sent to the **Control Center** as compared to when you select **Report** on virus detection.

Set the **Restart computer automatically**[] flag to reboot user's computer automatically after the scan is completed, if during the check infected objects detected and the cure process requires reboot of operating system. If the flag is cleared, reboot of a user's computer is not performed. Statistics of a station scan received by the **Control Center**, contains notification on the need of station reboot to compete the cure process. Information on a state that requiring reboot is displayed in the State table. Administrator is able to reboot a station from the **Control Center** if it is needed (see the Anti-Virus Network section).

Set the **Show scan progress** flag to display a progress bar and the status bar of the stations scan process in the **Control Center**.

6.5.4.3. Limitations

Settings that are not supported in check of stations under UNIX system-based and MAS OS X are marked with the [] sign.

In the Limitations section, the following settings are available:

- **Maximum scanning time (ms)** - maximal scanning time of one object in milliseconds. When the specified time expires, the scan of this object is interrupted.
- **Maximum archive nesting level** - maximal number of nested archives. If the maximum nesting level for archived files exceeds specified value, the scan performs until specified nesting level only.
- **Maximum archive size (KB)**[] - maximal size of scanned archive in kilobytes. If the archive size exceed the limit, neither unpacks, nor scans performed.
- **Maximum compression ratio** - maximal archives compression rate. If the **Scanner** defines what compression rate of the archive exceed specified limit, neither unpacks, nor scans performed.
- **Maximum size of extracted files (KB)**[] - maximal file size at unpacking. If the **Scanner** defines what the size of files after extracting the archive will exceed specified limit, neither unpacks, nor scans performed.
- **Compression check threshold (KB)**[] - minimal size of file inside archive beginning from which compression ratio check is performed.

6.5.4.4. Exclusions

In the **Exclusions** section, you can specify the list of files and folders to exclude from the anti-virus check.

To edit lists of files and paths excluded from scan

1. In the **Excluded paths and files** line, specify a path to corresponding file or folder.
2. To add a new line, click , and specify a path in the new line.
3. To remove a path from the list, click next to the corresponding line.

The list of paths excluded from the scan can contain the following elements:

1. Direct path in the explicit form to the excluded object. And:
   - A character \ or / excludes the entire disc with the Windows OS installation folder,
   - A character \ at the end of a path excludes the folder from checking,

- A path without a character `\` at the end - all subfolders of the selected folder are excluded from checking,

For example: `C:\Windows` - skip scanning files of the `C:\Windows` folder and all its subfolders.

2. Masks of objects, excluded from the scan. The `?` and the `*` symbols can be used to specify masks.

   For example: `C:\Windows\*\*.dll` - `C:\Windows`. skip scanning all files with the `dll` extension at all subfolders of the `C:\Windows` folder.

3. Regular expression. Paths can be specified through regular expressions. Any file those full name (with the path) corresponds to a regular expression is excluded from checking.

Before starting **Dr.Web Scanner for Windows** familiarize yourself with recommendations on virus scanning for computers operated by Windows Server 2003 OS, Windows 2000, or Windows XP OS. The information can be found at http://support.microsoft.com/kb/822158/en. The article is meant to help you increase system performance.

The syntax of regular expressions used for excluding paths from scanning is as follows:
`qr{expression}flags`

As a flag mostly the character `i` is used. It instructs "to ignore letter case difference".

Some examples of specifying excluded paths through regular expressions are given below:

- `qr{\\pagefile\.sys$}i` – skip scanning Windows NT swap files,
- `qr{\\notepad\.exe$}i` – skip scanning `notepad.exe` files,
- `qr{^C:}i` – skip scanning disk C,
- `qr{^.:\\WINNT\\}i` – skip scanning `WINNT` catalogs on all disks,
- `qr{(^C:)|(^.:\\WINNT\\)}i` – skip scanning disk `C` and `WINNT` catalogs on all disks,
- `qr{^C:\\dir1\\dir2\\file\.ext$}i` – skip scanning the `c:\dir1\dir2\file.ext` file,
- `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` – skip scanning `file.ext`, if it is located in the `c:\dir1\dir2` catalog and its subcatalogs,
- `qr{^C:\\dir1\\dir2\\}i` – skip scanning `c:\dir1\dir2` and its subcatalogs,
- `qr{dir\\^\\+}i` – skip scanning the `dir` subcatalog located in any catalog, but scan its subcatalogs,
- `qr{dir\\}i` – skip scanning the `dir` subcatalog located in any catalog and its subcatalogs.

Regular expressions briefly described in the **Appendices** document, in the Appendix J. Regular Expressions Used in Dr.Web Enterprise Security Suitesection.

In the **Scan contents of the following files** subsection, you can disable the check of compound objects. For this, clear the following flags:

- The **Archives** flag instructs the **Scanner** to search for viruses in files within archives.
- The **Email files** flag instructs to scan mailboxes.
- The **Installation packages** flag instructs the **Scanner** to search for viruses in packages for program installation.

6.6. Viewing Workstation Statistics

Via the control menu of the **Anti-virus network** section, you can view the following information:

- Statistics - to view data on anti-virus components functioning at the stations, stations and anti-virus components status, to view and save the reports, that contains all statistic data or selective statistic tables.
- Charts - to view charts with information on infections, detected at the stations.
- Quarantine - remote access to the **Quarantine** contents at the station.

6.6.1. Statistics

To view tables:

1. Select the **Anti-virus network** item in the main menu of the **Control Center** and in the opened window, click the name of the station or group in the hierarchical list.
2. In the opened control menu, select a necessary item in the **Statistics** section.

The **Statistics** section of the menu contains the following items:

- **Summary statistics** - view full statistics which is not divided into sessions.
- Summary data - view and save the reports, that contains all statistic data or selective statistic tables. This menu item will not be displayed if all other menu items are hidden in the **Statistic** section.
- **Threats** - view information on virus events (list of infected objects, viruses, anti-virus actions, etc.).
- **Errors** - view a list of scanning errors on a selected workstation for a certain period.
- Scan statistics - view statistics on the operation of anti-virus facilities on a workstation.
- **Start/Stop** - view a list of components which operated on a workstation.
- **Threat statistics** - view information on viruses detected on a workstation which are grouped by type.
- Status - view data on an unusual state of workstations, which might need your attention.
- **Tasks** - view the list of tasks set for a workstation during a certain period.
- **Products** - view information on products installed on selected stations. In this case, products refers to the **Server** repository products.
- **Virus bases** - view details on installed virus databases including information on the file containing a particular database, virus database version, the total number of virus records in the database, the database creation date. This menu item is available only if stations selected.
- **Modules** - view detailed information on all **Dr.Web** modules including module description - its function name, the executable file for the separate product, the full module version etc. This menu item is available only if stations selected.
- **All network installations** - view a list of **Agent** installations on a workstation or group of workstations.
- **All deinstallations** - view the list of workstations with deinstalled **Dr.Web** anti-virus software.

To show hidden items of the **Statistics** section, select **Administration** in the main menu, then in the opened window select **Dr.Web Server configuration** in the control menu. On the **Statistics** tab, set corresponding flags (see below), then click **Save** and restart the **Server**.

Table 6-8. Correspondence between items of Statistics section and flags of Statistics data section

Statistics section items	Flags from the Statistic section of the Server configuration
Summary statistics	Scan statistics

Statistics section items	Flags from the Statistic section of the Server configuration
Threats	Detected security threats
Errors	Scan errors
Scan statistics	Scan statistics
Start/Stop	Start/Stop of components
Threat statistics	Detected security threats
Status	Station statuses
Tasks	Station tasks execution log
Virus Bases	Stations statuses Virus database statuses Station tasks execution log
Modules	List of the station modules
All network installations	Agent installations

The windows with the statistics for different components and the total statistics of workstations have the same interface, and the actions to set the information to be provided are similar.

Below several examples for viewing the statistics via **Dr.Web Security Control Center** are given.

6.6.1.1. Summary Data

To view Summary data:

1. In the hierarchical list select a station or a group.
2. Select **Summary data** item from the **Statistics** section of the control menu.
3. The window with report table data will be opened. To include specific data in the report, click **Summary data** on the toolbar and select necessary types in the drop-down list: **Scan statistics**, **Threats**, **Tasks**, **Start/Stop**, **Errors**. Statistics from this report sections are similar to statistics from the corresponding items of the **Table** section. To view the report with selected tables, click **Refresh**.
4. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.
5. To save the report for printing or future processing, click one of the following buttons:
   - **Save data in CSV file**,
   - **Save data in HTML file**,
   - **Save data in XML file**,
   - **Save data in PDF file**.

6.6.1.2. Scan Statistics

To view the statistics on operation of anti-virus programs on a workstation

1. In the hierarchical list select a station or a group.

> If you want to view records for several stations or groups, select these stations keeping the SHIFT or CTRL key pressed.

2. In the control menu select **Scan Statistics** item from the **Statistics** section.

3. The Statistics window will be opened. The statistics for last 24 hours are displayed by default.
4. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**. The tables with statistics will be loaded.
5. In the **Summary statistics** section, the summary data is displayed:
   - if stations are selected - by selected stations;
   - if groups are selected - by selected groups. If several groups are selected, only non-empty groups will be displayed;
   - If both stations and groups are selected - separately by all stations, including stations from selected non-empty groups.
6. To view the detailed statistics of anti-virus components, click the station name in the table. If groups were selected, click the group name in the summary statistics table, then click the station name in the displayed table. A windows (or a section of current window) with detailed statistics will be opened.
7. You can open the settings window of the anti-virus component from the statistic table of station or group components. To do this, click the name of the component in the statistic table.
8. To sort the data in columns of a table, click the certain point (decrease or increase) in the header of the table.
9. To save the table for printing or future processing, click one of the following buttons:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.
10. To view the summary statistics not split in sessions, click **Summary statistics** in the control menu. A window of summary statistics will be opened.
11. To view the statistics as a charts, click **Charts** in the control menu. A statistics charts window will be opened (see detailed description below).

6.6.1.3. Status

To view data on workstations status:

1. In the hierarchical list select a station or a group.
2. In the control menu select **Status** item from the **Statistics** section.
3. Status information are displayed according to the filter settings. Click on the toolbar, to change the following filter parameters:
   - In the **Period** drop-down list, select a time period during which stations have not been connected to the **Server**. Period field displays the number of days corresponding to the selected period: the list will contain stations which have been disconnected from the **Server** during specified time slot or more. In case of excess of this count, situation is rated as critical for the anti-virus network security.
   - In the **Severity** drop-down list, set the flags for necessary levels of messages severity: the list of messages on status will contain only messages with selected severity. All flags are set by default.
   - In the **Source** list, set the flags for those sources of messages appearance that will be displayed in the list:
     - **Agent** - display events from **Dr.Web Agents** connected to this **Server**.
     - **Server** - display events from this **Dr.Web Server**.
   - In the **Stations** list, set the flags for stations status types, messages on which will be displayed in the list:
     - **Online** - display events for stations which are connected to this **Server** and currently online.
     - **Offline** - display events for stations which are connected to this **Server** and currently offline.
     - **Deinstalled** - display the last event for stations with deinstalled **Dr.Web** anti-virus software.
4. To manage filter settings, use the following buttons on the filter pane:
   - **Default** - set the default values to all filter settings.
   - **Refresh** - apply selected filter settings.
5. You can format the way the data are presented just like in the statistics window above.

To view operation results and statistics for several workstations, select those workstations in the network hierarchical list.

6.6.2. Charts

Infection Charts

To view general charts with information on detected infections:

1. Select **Anti-virus network** in the main menu of the **Control Center**, then in the opened window in the hierarchical list click the station or group name. In the opened control menu in the **General** section, select **Charts**.
2. Window with the following charts will be opened:
   - **Viral activity** - chart displays the total number of malware detected per each time slot at all selected stations and groups. The chart is displayed if specified time period exceeds 24 hours.
   - **Most common threats** - displays the list containing ten threats that are met in the most of files. The chat displays numerical data on objects which correspond to the specific threat.
   - **Threat classes** - displays the list of threats corresponding to the malware specification. The pie chart displays percentage between all of detected threats.
   - **Most infected stations** - displays the list of stations on which security threats detected. Chart displays the total number of threats for each stations.
   - **Actions performed** - displays the list of actions performed to detected malware. The pie chart displays percentage between all of performed actions.
3. To view data for a certain time slot, specify it in the drop-down list on the toolbar: view the certain day or month. Or you can select the arbitrary date range. To do this, enter required time and date or click the calendar icons to set the time period. To view the data, click **Refresh**.
4. To exclude an item from displaying on a chart (except the **Viral activity** chart), click the name of this item in the legend under the chart.

Total Statistics Charts

Graphical data is displayed in the **Charts** entry of the **General** section and in some entries of the **Statistics** section.

Depending on the object, selected in the hierarchical list (station or group), different collections of charts are displayed. In the table below, charts and sections of the control menu, in which these charts are displayed, are listed.

Table 6-9. Correspondence between charts, items selected in the hierarchical list and sections of the control menu

Charts	For groups	For stations	Sections
Viral activity	+	+	Charts
Most common threats	+	+	Charts Threats Threat statistics
Threat Classes	+	+	Charts Threat statistics
Most infected stations	+	+	Charts
Actions performed	+	+	Charts Threats
Count of errors by stations	+	+	Errors
Count of errors by components	+	+	Errors

Charts	For groups	For stations	Sections
Threats by components	+	+	Start/Stop
Errors by components	+	+	Start/Stop

- **Count of errors by stations** - displays the list of stations on which errors in anti-virus components operation detected. Graph displays the total number of errors for each station.
- **Count of errors by components** - displays the list of anti-virus components in which operation errors detected. The pie chart displays percentage between errors of all components.
- **Threats by components** - displays the list of anti-virus components which detected the threats. Chart displays the total number of threats detected by each component.
- **Errors by components** - displays the list of anti-virus components in which operation errors detected. Chart displays the total number of errors for each component.

6.6.3. Quarantine

Quarantine Content

Files can be added to the **Quarantine**:

- by one of anti-virus components, e.g. **Scanner**,
- manually by user via the **Quarantine** Manager.

After moving to **Quarantine**, files are automatically rescanned. This affords:

- clarifies the status of infection: presence of infection and its type (because in manual moving to **Quarantine**, information on files infection status is unavailable),
- infection names and their type are cast to a common view.

Also, user can rescan files in **Quarantine** via the **Control Center** or via the **Quarantine** Manager at the station.

To view and manage Quarantine via the Control Center:

1. Select the **Anti-virus network** item in the main menu, then click the name of the station or group in the hierarchical list and select **Quarantine** in the control menu.
2. A new window with table that contains **Quarantine** current state opens. If you selected one workstation, a table in the window displays objects in **Quarantine** at this station. If you selected more than one stations or one or more groups, the windows displays a set of tables with quarantined objects for each station.
3. To filter files by time when they were quarantined, set a time slot on the toolbar and click **Refresh**.
4. To manage files in **Quarantine**, set the flag for the corresponding file, group of files or for all files in the **Quarantine** (at the table header). On the toolbar, select one of the following actions:
   - - Restore the files from the **Quarantine**.

     Use this option only if you are sure that objects are harmless.

     Select one of the options from the drop-down list:

     a) - Restore the original location of the file, i.e. restore the file to the folder where it had resided before it was moved to the **Quarantine**.

     b) - Restore the file to the folder specified by the administrator.
   - **Remove files** - delete the file from the **Quarantine** and from the system.

- **Scan files** - scan selected in **Quarantine** file one more time.
- **Export** - copy and save selected in **Quarantine** files.

After moving suspicious files to the local **Quarantine** on user's computer, you can copy these files via the **Control Center** and save them via the web browser, e.g. to send files to **Dr.Web virus laboratory** ulteriorly. For saving, set the flags for the needed files and click **Export**.

- Export data about the **Quarantine** state to a file in one of the following formats:

Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

6.7. Mailing of Installation Files

After a new stations account is created in the **Control Center**, the installation package for **Dr.Web Agent** installation is generated. Installation package contains the **Anti-virus** installer and the set of parameters for connecting to the **Server** and for authorization of the station at the **Server** (description of installation package and the process of **Agent** installation via this package is given in the **Installation Manual**, in the Local Installation of Dr.Web Agent section).

After the installation package is created, for the convenience of their distribution, you can sent specific installation packages to the user's email.

To send installation packages, the email content is formed by the following way:

1. Operating system of the station is known:
   a) Windows OS: the letter attachment contains **Dr.Web Agent for Windows** installation package.
   b) Linux OS, OS X, Android OS: the letter attachment contains **Dr.Web Agent** installation package for the corresponding operating system and the configuration file with the settings for connecting to **Dr.Web Server**.
2. Operating system of the station is unknown (the new station account, **Agent** in not yet installed):
   a) If the **Server** does not contain the packages for stations under Linux OS, OS X, Android OS (in particular, the extra distribution kit of the **Server** is not installed): the letter attachment contains **Dr.Web Agent for Windows** installation package and the configuration file with the settings for connecting to **Dr.Web Server** for stations under Linux OS, OS X, Android OS.
   b) If the **Server** contains at least one package except packages for stations under Windows OS: the letter attachment contains **Dr.Web Agent for Windows** installation package, the configuration file with the settings for connecting to **Dr.Web Server** for stations under Linux OS, OS X, Android OS and the link to download installation packages for stations under Linux OS, OS X, Android OS.

To email installation package:

1. Select the **Anti-virus network** item in the main menu of the **Control Center** and in the opened window, select the following objects in the hierarchical list:
   - select the station to email the installation package generated for this station.
   - select the group of stations to email all installation packages generated for stations of this group.

   Use CTRL or SHIFT to select several objects at at time.
2. On the toolbar, click **General** → **Mail installation files**.
3. In the **Mailing of installation files** opened section, specify the following parameters:

- In the **Recipient email addresses** section, specify the email address to sent installation package to. If several stations or groups were selected, specify email addresses to send installation packages of each station separately next to this station name.
- In the **Additional** section, set the **Pack in zip archive** flag to pack installation packages into a zip archive. Archiving can be useful if the user's email system contains filters that block sending of executable files in emails attachment.
- In the **Sender** section, specify the email address which will be set as a sender of the email with installation files.
- In the **SMTP server settings** section, you can specify SMTP server parameters which will be used to send email. In the parameters are known, e.g. already been specified, this section will be folded, you can unfold it and edit specify parameters, if necessary. At first sending of installation packages, in the opened section you must specify the following parameters:
  - **Address** – SMTP server address which is used to send emails.
  - **Port** – SMTP server port which is used to send emails.
  - **User**, **Password** (**Retype password**) – if necessary, specify name and password of SMTP server user, if the SMTP server requires authorization.
  - Set the **STARTTLS encoding** flag to use *STARTTLS* traffic encoding for sending messages on email.
  - Set the **SSL encoding** flag to use *SSL* traffic encoding for sending messages on email.
  - Set the **Use CRAM-MD5 authentication** flag to use *CRAM-MD5* authentication on a mail server.
  - Set the **Use DIGEST-MD5 authentication** flag to use *DIGEST-MD5* authentication on a mail server.
  - Set the **Use the plain authentication** flag to use *plain text* authentication on a mail server.
  - Set the **Use LOGIN authentication** flag to use *LOGIN* authentication on a mail server.
  - Set the **Validate the SSL server certificate** flag to enable validating the SSL certificate of a mail server.
  - Set the **Debug mode** flag to get SMTP session detailed log.Click **Send**.

6.8. Sending Notifications to Users

The system administrator may send the users informational messages including:

- message text;
- hyperlinks to Internet resources;
- company logo (or any other graphic presentation);
- exact date of message receipt in the title of the window.

These messages are displayed on user's PC as popup windows (see figure 6-1).

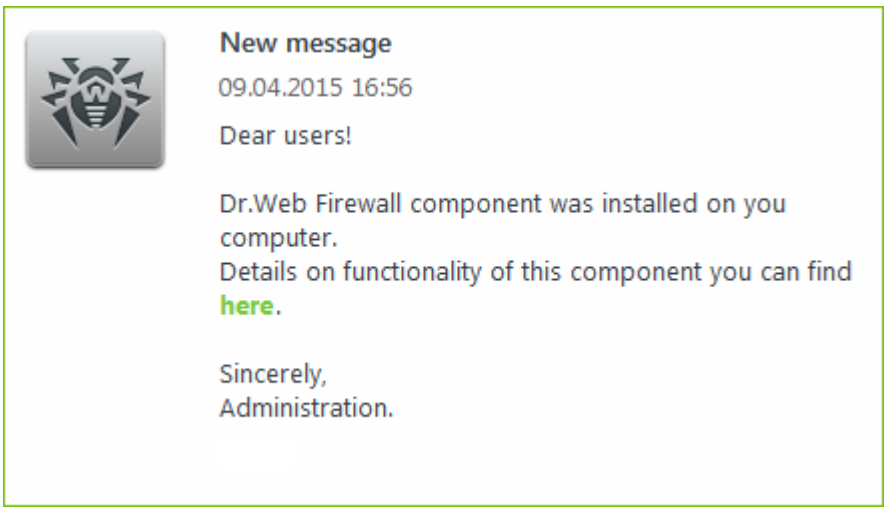


Figure 6-1. Message window on user's PC

To send a message to a user

1. Select the **Anti-virus network** item in the main menu of the **Control Center**.
2. In the opened window, select a station or a group in the hierarchical list and click **General** → **Send message** on the toolbar.
3. Specify the following fields in the opened window:
   - **Message text** – an obligatory field containing the message itself.
   - Set the **Show logotype in the message** flag, to display a graphical object in the message window title. Specify the following logotype parameters:
     - Set the **Use transparency** flag to use a transparency in the logotype image (see Logo File Format, p. 4).
     - In the **URL** field, you can specify the link to an Internet resource to open on the logo and message title click.
     - In the **Message title** field, you can specify the title of the message, e.g. the company name. This text will be displayed in the message window title on the right of the logo. If you leave this field blank, information on the message will be displayed in the title of the message window.
     - On the right of the **Logotype file** field, click to load the logotype file from the local resource, and select the necessary object in the opened file system browser.

   If the logotype is not set or the logotype size exceeds the allowable limits (see Logo File Format, p. 3), **Dr.Web Agent** logotype will be displayed in its place in the message window.
   - Set the **Show link in the message** flag, to include a hyperlinks to web resources into the message.

   To insert a link:
   1. In the **URL** field, specify a link to an Internet resource.
   2. In the **Text** field, specify the link name - a text displayed in the link place in the message.
   3. In the **Message text** field, add the `{link}` marker in all places where you want the link to appear. In the resulting message, the link with the specified parameters will be shown instead of the marker. You may use unlimited number of the `{link}` markers in a text, all of them will have the same parameters from the **URL** and **Text** fields.
   - Set the **Send to online stations only** flag to send the message to online stations only. If the flag is set, sending to offline stations is not performed. If the flag is cleared, sending to offline stations is postponed till their connection.
   - Set the **Show send status** flag, to show notification with the message send status.
4. Click **Send**.

Logo File Format

A file with graphic image (logotype) inserted into a message should require the following:

1. File graphic format: BMP, JPG, PNG, GIF, SVG.
2. Logo file size may not exceed 512 KB.
3. Overall image size is 72x72 pixels. Images of other size will be scaled to the default size before send.
4. Bit depth is any (8 - 24 bit).
5. If the **Use transparency** flag is set when sending a message, the first pixel in the position (0,0) is declared *transparent*. All pixels of the same colour as the initial colour of this pixel become transparent, the window background is be displayed instead.

   If you use the **Use transparency** option for rectangular logotype, it is recommended to make a rectangular border to avoid erroneous transparency of the pixels of the image itself.

   Enabling the **Use transparency** option will be useful in case of a nonstandard (non-rectangular) form of the logotype to remove the undesirable background, which supplements the informative part of the image to a rectangular shape. For example, if the image shown in figure 6-2 is used as a logotype, the purple background will be removed (become transparent).

Figure 6-2. Nonstandard form logotype

If you want to use transparent background logotype in the message, use the PNG or GIF file formats.

Before sending a user message (especially to multiple users), it is recommended to send it first to any computer with the **Agent** installed to check the adequacy of the result.

Message Send Example

To send the message displayed in figure 6-1, the following parameters were set for the link:

Message text:

```
Dear users!

Dr.Web Firewall component was installed on you computer.
Details on functionality of this component you can find {link}.

Sincerely,
Administration.
```

URL: `http://drweb.com/`

Text: `here`

Chapter 7: Configuring Dr.Web Server

This chapter contains a description of the following features for managing operation parameters of the anti-virus network and **Dr.Web Server**:

- Logging - view the operation log of the **Server**, view detailed statistic data on the **Server** operation;
- Setting Dr.Web Server Configuration - configure **Server** operation parameters;
- Setting Dr.Web Server Schedule - configure scheduled tasks to maintain the **Server**;
- Setting the Web Server Configuration - configure **web server** operation parameters;
- User Hooks - enable and configure user hooks;
- Setting Notifications - configure the system of administrator notifications about anti-virus network events with different methods of notification delivering;
- Administration of Dr.Web Server Repository - configure repository to update all anti-virus network components from the **GUS** and further propagation of updates on stations;
- Database Management - direct maintenance of the **Server** database;
- Peculiarities of a Network with Several Dr.Web Servers - configure multiserver anti-virus network and the neighbor connections.

7.1. Logging

7.1.1. Audit Log

Audit log allows to view the list of events and changes carried via the control subsystems of **Dr.Web Enterprise Security Suite**.

To view the audit log:

1. Select the **Administrating** item in the main menu of the **Control Center**.
2. In the opened window, select the **Audit log** item of the control menu.
3. Window with the registered actions table opens. To configure viewing the log, specify on the toolbar the time period during which the actions have been performed. For this, you can select one of the proposed periods or specify arbitrary dates in the calendars which are opened on clicking the dates fields. Click **Refresh** to display the log for the selected dates.
4. The log table contains the following data:
   - **Date** - date and time when the action has been performed.
   - **Login** - login of the **Server** administrator. It is specified if the action was initiated directly by administrator or during connection to the **Server** according to the administrator credentials.
   - **Address** - IP address from which the action execution has been initiated. It is specified only in case of an external connection to the **Server**, particularly via the **Control Center** or via the Web API.
   - **Subsystem** - the name of the subsystem by which or via which the action has been initiated. The audit is logged for the following subsystems:
     - **Control Center** - the action was performed via **Dr.Web Security Control Center**, particularly by administrator.
     - **Web API** - the action was performed via the *Web API*, e.g., from an external software connected according to the administrator credentials (see also the **Appendices** document, p. Appendix L. Integration of Web API and Dr.Web Enterprise Security Suite).
     - **Server** - the action was performed by **Dr.Web Server**, e.g., according to its schedule.
     - **Utilities** - the action is initiated via the external utilities, particularly via **Dr.Web Server remote diagnostics utility**.

- **Result** - the brief result of the action performing:
  - **OK** - operation successfully executed.
  - **failed** - an error occurred during the operation execution. Operation is not executed.
  - **initiated** - operation execution is initiated. The result of operation execution will be known just after its completion.
  - **no rights** - administrator that launched the operation execution has no permissions to execute this operation.
  - **delayed** - action execution is postponed until a certain period or performing of a certain event.
  - **not allowed** - execution of the requested action is prohibited. For example, deleting of system groups.

Lines that correspond to actions executed with an error (the **failed** value in the **Result** column), are marked with red.

- **Operation** - the action description.

5. If necessary, you can export data for the specified period into a file. To do this, click on the the following buttons on the toolbar:

Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

7.1.2. Dr.Web Server Logging

Dr.Web Server logs the events connected with its operation. Its name is `drwcsd.log`.

The **Server** log helps to detect the problem in case of an abnormal operation of **Dr.Web Enterprise Security Suite** anti-virus.

The log file resides by default:

- Under **UNIX** OS:
  - for Linux OS and Solaris OS: `/var/opt/drwcs/log/drwcsd.log`;
  - for FreeBSD OS: `/var/drwcs/log/drwcsd.log`.
- Under **Windows** OS: in the `var` subfolder of the **Server** installation folder.

It is a plain text file (see the **Appendices** document, the Appendix K. Log Files Format section).

To view the Server log via the Control Center:

1. Select the **Administrating** item in the main menu of the **Control Center**.
2. In the opened window, select the **Dr.Web Server log** item of the control menu.
3. Window with the **Server** logs list opens. According to the rotation mode settings, the following names format of **Server** log files is used: *<file_name>*.*<N>*.`log` or *<file_name>*.*<N>*.`log.gz`, where *<N>* - sequence number: 1, 2, etc. E.g, if the log file name is `drwcsd`, the list of log files is the following:
   - `drwcsd.log` – current log file,
   - `drwcsd.1.log` – previous log file,
   - `drwcsd.2.log` and so on – the greater the number, the older the version of the log.

4. To manage log files, set the flag next to the necessary file or several files. To select all log files, set the flag in the header of the table. On the toolbar, the following buttons become available:

   Export selected log files - save local copy of selected log files. It can be useful, e.g. to view the log file content from the remote computer.

   Delete selected log files - delete selected log files without possibility to restore.

7.1.3. Repository Updates Log

Repository updates log allows to view the list of updates from **GUS**, that includes detailed information on updated products revisions.

To view the repository updates log:

1. Select the **Administrating** item in the main menu of the **Control Center**.
2. In the opened window, select the **Log of repository updates** item of the control menu.
3. Window with the registered actions table opens. To configure viewing the log, specify on the toolbar the time period during which the actions have been performed. For this, you can select one of the proposed periods or specify arbitrary dates in the calendars which are opened on clicking the dates fields. Click **Refresh** to display the log for the selected dates.
4. The log table contains the following data:
   - **Start** - date and time when an update of the certain product has been started from the **GUS**.
   - **Finish** - date and time when an update of the certain product has been finished from the **GUS**.
   - **Product name** - name of the repository product that was downloaded or was requested to be downloaded.
   - **Update result** - repository update result. Contains brief information on successful update completion or error reason.

The **Update result** cells that correspond to actions executed with an error, are marked with red.

   - **Initial revision** - number of the revision (revisions are numbered according to the date of their creation) that was the last for this product before update process started.
   - **Revision from update** - number of the revision (revisions are numbered according to the date of their creation) that was was downloaded during update process.
   - **Updated files** - brief information on the changed files. Is given in the following format: *<files number> – <actions on files>*.
   - **Initiator** - system that initiated the update process:
     - **Launched from the command line** - update was initiated by administrator via the corresponding console command.
     - **Launched by Task Scheduler** - update wad launched according to the task in the Dr.Web Server schedule.
     - **Interserver update** - update was received via the interserver connection from the main **Server**. This initiator presents only in case of multiserver configuration of anti-virus network with propagation of update via the interserver connections.
     - **Launched from the Control Center** - update was launched by administrator via **Dr.Web Security Control Center**, from the Repository State section.
     - **Repository import** - update was loaded by administrator in the Repository Content section of the **Control Center**.
   - **Administrator** - login of the **Server** administrator. It is specified if the action was initiated directly by administrator.

- **Network address** - IP address from which the action execution has been initiated. It is specified only in case of an external connection to the **Server**, particularly via the **Control Center** or via the Web API.
- **Repository folder** - folder name of the **Server** repository that was modified according to the update process.

5. To view the detailed information on a certain update, click the line of this update. This opens the window with table on product files changed during selected update. The following information is given fro each file: **File name**, **File hash**, **Size** and **State**.
6. If necessary, you can export data for the specified period into a file. To do this, click on the the following buttons on the toolbar:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.

7.2. Setting Dr.Web Server Configuration

To set the configuration parameters of Dr.Web Server:

1. Select the **Administration** item in the main menu of the **Control Center**.
2. Select **Dr.Web Server configuration** in the control menu. A window with **Server** configuration will be opened.

Values of fields, marked by the * sign, must be obligatory specified.

3. On the toolbar, the following buttons to manage the section settings are available:

   Restart Dr.Web Server - restart the **Server** to apply changes that have been specified in this section. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Restore configuration from the backup - drop-down list with the backup of all section settings, which you can restore after making changes. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Reset all parameters to initial values - restore the values that all parameters in this section had before current editing (last saved values).

   Reset all parameters to default values - restore default values of all parameters in this section.
4. To apply the changes specified in the section settings, click **Save**, after this the **Server** must be rebooted. To do this, click **Restart Dr.Web Server** on the toolbar of this section.

7.2.1. General

On the **General** tab, you can configure the following **Server** parameters:

- **Dr.Web Server name** – the name of the **Server**. If it is not specified, the name of the computer where **Dr.Web Server** software is installed is used.
- **Parallel requests number** – the threads number processing data from the **Agents**. This parameter affects **Server** performance. Change the default setting on advice of the technical support only.
- **DB connections** – the number of database connections with the **Server**. Change the default setting on advice of the technical support only.

Starting from the **10.0** version, the **Authorization queue** parameter cannot be edited vie the **Control Center**.

On the new **Server** installation, this parameter takes the 50 default value. On the upgrade from the previous version saving configuration file, the authorization queue value is saved from the previous version configuration.

If you need to edit the authorization queue value, edit the following parameter value in the **Server** configuration file:

```
<!-- Maximun authorization queue length -->
<maximum-authorization-queue size='50'/>
```

- Set the **Limit updates traffic** flag to limit the network traffic bandwidth for transmitting updates from **Server** to **Agents**.

  If the flag is set, specify in the **Maximal transmission speed (KB/s)** field the value of maximal speed for updates transmission. Updates will be transferred in ranges of specified bandwidth of summary network traffic for all **Agents** updates.

  If the flag is cleared, updates for **Agents** are transferred without limitation of network traffic bandwidth.

  For more details see Update Traffic Limitations.

- In the **Newbies registration mode** drop-down list, select the registration mode for new stations (see New Stations Approval Policy).
  - In the **Default primary group** drop-down list select the group which is set as a primary when access of stations to the **Server** is allowed automatically.
- Set the **Reset unauthorized to newbie** flag to reset parameters to access the **Server** for workstations which have not passed authorization check. This option can be helpful when you change **Server** settings (such as public key) or change the DB. In such cases workstations will not be able to connect to the **Server** and will need to get the new parameters to assess the **Server**.
- In the **Encryption** drop-down list, select the policy of traffic encryption between **Dr.Web Server** and connected clients: **Dr.Web Agents**, neighbor **Servers**, **Network Installers**.

  For more details on this parameters, read p. Traffic Encryption and Compression.

- In the **Compression** drop-down list, select the policy of traffic compression between **Dr.Web Server** and connected clients: **Dr.Web Agents**, neighbor **Servers**, **Network Installers**. For more details on this parameters, read p. Traffic Encryption and Compression.
  - When you select **Yes** or **Possible** for traffic compression, the **Compression level** drop-down list become available. In this list you can select data compression level from 1 to 9, where the 1 is minimal level and 9 is maximal compression level.
- In the **Allowed difference between time of Server and Agent** field specify allowed difference between system time at **Dr.Web Server** and **Dr.Web Agents** in minutes. If the difference is larger than specified value, it will be noted in the status of the station at **Dr.Web Server**. 3 minutes are allowed by default. The 0 value means that checking is disabled.

- Set the **Replace IP addresses** flag to replace IP address with DNS names in **Dr.Web Server** log file.
- Set the **Replace NetBIOS names** flag to display DNS names instead of NetBIOS names in the catalog of the anti-virus network (when host names cannot be detected, IP addresses are displayed).

Replace IP addresses and **Replace NetBIOS names** flags are cleared by default. If the DNS service is not set up properly, enabling these flags may considerably slow down the **Server** operation. When using any of these options, it is recommended to enable cashing names on the DNS server.

If the **Replace NetBIOS names** flag is set and anti-virus network contains the **Proxy server**, when for all stations connected to the **Server** via the **Proxy server**, in **Dr.Web Security Control Center**, the name of computer on which the **Proxy server** is installed, will be shown instead of stations names.

- Set the **Synchronize stations descriptions** flag to synchronize stations descriptions with the description in **Dr.Web Security Control Center** (**Computer description** field at the **System properties** page). If the station description in **Dr.Web Security Control Center** is absent, the user description will be set to this field. If descriptions differ, the description in **Dr.Web Security Control Center** will be replaced by the user description.
- Set the **Track epidemic** flag to enable the mode of administrator notification on virus epidemic cases. If the flag is cleared, notifications on virus infection are performed in the standard mode. If the flag is set, you can configure the following parameters of virus epidemic tracking:
  - **Period (sec.)** - time period in seconds, during which specified number of messages on infections must be received, so that **Dr.Web Server** may send to the administrator a single notification on epidemic on all cases of infection.
  - **Messages number** - the number of messages on infections that must be received in specified time period, so that **Dr.Web Server** may send to the administrator a single notification on epidemic on all cases of infection.
- Set the **Synchronize geolocation** flag to enable synchronization of stations geolocation between **Dr.Web Servers** in multiserver anti-virus network. If the flag is set, you can configure the following parameter:
  - **Startup synchronization** - number of stations without geographical coordinates, information on which is requested when establishing a connection between **Dr.Web Servers**.

7.2.1.1. Traffic Encryption and Compression

Dr.Web Enterprise Security Suite anti-virus network allows encrypting the traffic between **Dr.Web Server** and workstations (**Dr.Web Agents**), between **Dr.Web Servers** (in multi-server anti-virus network configuration) and between **Dr.Web Server** the **Network Installers**. This mode is used to avoid leakage of user keys and also information on environment and anti-virus network users during components interaction.

Dr.Web Enterprise Security Suite anti-virus network uses reliable tools of encryption and digital signature based on the concept of pairs of public and private keys.

The encryption policy is set separately for each component of the anti-virus network, at this, settings of other components should be compatible with the settings of the **Server**.

As traffic between components, in particular the traffic between **Dr.Web Servers**, can be considerable, the anti-virus network provides for compression of this traffic. The setting of the compression policy and the compatibility of settings on different components are the same as those for encryption.

When configuring encryption and compression on the **Server**, please consider the features of the clients which are planning to be connected to this **Server**. Not all clients support traffic encryption and compression (e.g, **Dr.Web Anti-virus for Android** and **Dr.Web Anti-virus for OS X** do not support neither encryption nor compression). Such clients will not be able to connect to the **Server**, if the **Yes** value is specified for encryption and/or compression on the **Server**.

To set the encryption and compression policies for Dr.Web Server:

1. Select the **Administration** item in the main menu.
2. Click **Dr.Web Server configuration** in the control menu.
3. On the **General** tab, select the necessary variant in the **Encryption** and **Compression** drop-down lists:
   - **Yes** – enables obligatory traffic encryption (or compression) with all components (is set by default for encryption, if the parameter has not been modified during the **Server** installation),
   - **Possible** – instructs to encrypt (or compress) traffic with those components those settings do not prohibit it,
   - **No** – encryption (or compression) is not supported (is set by default for compression, if the parameter has not been modified during the **Server** installation).

When coordinating the settings of the encryption policy on the **Server** and other components (the **Agent** or the **Network Installer**), one should remember, that certain combinations are incompatible and, if selected, will result in disconnecting the corresponding component from the **Server**.

7-1 describes what settings provide for encryption between the **Server** and the components (**+**), when the connection will be non-encrypted (–) and what combinations are incompatible (**Error**).

Table 7-1. Compatibility of the encryption policy settings

Component settings	Server settings		
	Yes	Possible	No
Yes	+	+	Error
Possible	+	+	–
No	Error	–	–

Encryption of traffic creates a considerable load on computers those capacities are close to the minimal system requirements for the components installed on them. So, when traffic encryption is not required to provide additional security, you can disable this mode. Traffic encryption is also not recommended in big networks (more then 2000 clients).

To disable encryption mode, you should step by step switch the **Server** and other components to the **Possible** mode first, avoiding formation of incompatible **Network Installer-Server** and **Agent-Server** pairs. If you do not follow this recommendation it may result in loss of connection with the component and the necessity to reinstall it.

Using the compression mode reduces traffic, but considerably increases the computational load on computers, more than the encryption.

The **Possible** value in **Dr.Web Agent** settings means that by default the traffic will be encrypted/ compressed, but it can be disabled by editing the settings of the **Server** without editing the settings of the **Agent**.

7.2.1.2. Workstation Traffic Limitations

You can limit the network traffic bandwidth for transferring data between **Server** and **Agents** in **Dr.Web Enterprise Security Suite** anti-virus network. You can separately configure limitations for transferring updates and limitations for transferring data during **Agent** installations.

The following options to limit the data traffic are available:

1. Limit data transfer bandwidth for all workstations.

   You can configure this option in the **Server** configuration section: select the **Administration** item in the main menu of the **Control Center** → the **Dr.Web Server configuration** item in the control menu → the **General** tab → the **Updates** or **Installations** internal tab → the **Limit traffic** option.

2. Limit update transfer bandwidth for certain stations or groups of stations personally.

   You can configure this option in stations configuration section: select the **Anti-virus Network** item in the main menu of the **Control Center** → select the station or group of stations in the network hierarchical list → the **Traffic restrictions** item of the control menu → the **Updates** or **Installations** internal tab → the **Limit traffic** option.

Data traffic is limited as follows:

1. If limitation is enabled for the common rate of data transferring in the **Server** settings, the summary rate of transferring data from **Server** to all stations will not exceed the specified value. At that:
   a) Not depending on the difference in bandwidth of channels between **Server** and stations, the transfer rate is equally distributed among all the stations.
   b) If the bandwidth of a channel between **Server** and a station is less than the average rate for one station calculated according to the **a)** item, the data transferring traffic for this station is limited to the maximum bandwidth of this channel. The rest limit of the common rate, is equally distributed among the set of stations as described in the **a)** item.
2. If the personal limitation for data transferring rate is set for a certain station or group of stations, the rate of transferring data to this group or stations will not exceed the specified value. This limitation does not affect on other stations and data are transferred to them at the maximum rate.
3. If both common and personal limitations are set in the **Server** settings and in the settings of a certain station or group, when:
   a) Rate of transferring data to the personally limited groups and stations will not exceed the value specified in their settings.
   b) Rate of transferring data to the rest of stations is calculated as follows: the common limitation of data transferring rate, after subtraction of limitations in the **a)** item, is equally distributed among other workstations.
   c) If the bandwidth of a channel between **Server** and a station, for which no personal limit is specified, is less than the average rate obtained in the **b)** item, the traffic for this station is limited to the maximum bandwidth of this channel. The rest rate similarly to the **b)** item is equally distributed among other stations, for which no personal limitations are specified.

7.2.2. DNS

On the **DNS** tab, you can configure the following parameters of DNS server usage:

- **DNS queries timeout (sec.)** – timeout in seconds for resolving DNS direct/reverse queries. Set the 0 value to disable restriction on wait time until the end of the resolution.

- **Number of retried DNS queries** – maximum number of repeated DNS queries on fail while resolving the DNS query.
- Set the **Set the time to store DNS server responses** flag to specify time for storing responses from DNS server in the cache (TTL).
  - **For positive responses (min.)** – the storage time in the cache (TTL) of positive responses from the DNS server in minutes.
  - **For negative responses (min.)** – the storage time in the cache (TTL) of negative responses from the DNS server in minutes.
- **DNS servers** – List of DNS servers, which replaces default system list.
- **DNS domains** – List of DNS domains, which replaces default system list.

7.2.3. Statistics

On the **Statistics** tab you can configure statistics information to write in the log file and to the **Server** data base.

To add corresponding type of information to the DB, set the following flags:

- **Quarantine state** – logs stations **Quarantine** state.
- **Hardware and software composition** – enables monitoring of hardware and software composition and storing the information in the database.
- **List of the station modules** – enables monitoring of the list of the station modules and storing the information in the database.
- **List of installed components** – enables monitoring of the list of the installed components (**Scanner**, monitors, etc) and storing the information in the database.
- **Sessions of stations users** – enables monitoring of user sessions and storing in the database the logins of users which are loged in the system with installed **Agent**.
- **Start/Stop of components** – enables monitoring of the information on the start and stop of the components (**Scanner**, monitors, etc) and storing the information in the database at stations.
- **Detected security threats** – enables monitoring of infections detecting and storing the information in the database.

  If the **Detected security threats** flag is set, you can also configure additional parameters of statistic on infections.

  Set the **Send statistics to Doctor Web company** flag, to activate sending statistics on detected stations security threats to the **Doctor Web** company. The following fields will become available:

  - **Interval** – an interval in minutes for sending statistics;
  - **Identifier** – an MD5 key (located in the **Server** configuration file);

  Interval for sending statistics is the only obligatory field.

- **Scan errors** – enables monitoring of scan errors occurring and storing the information in the database.
- **Scan statistics** – enables monitoring of the statistics of scanning and storing the information in the database.
- **Agent installations** – logs the information about **Agent** installations at the stations.
- **Station tasks execution log** – log results of tasks execution on workstations and store the log in the DB.
- **Station statuses** – log status changes for workstations and store the log in the DB.
  - **Virus database statuses** – log changes in virus databases status and contents on workstations and store the logs in the DB.

To view statistics information:

1. Select the **Anti-virus network** item of the main menu.
2. Select a station or a group in the hierarchical list.
3. Open the corresponding section of the control menu (see the table below).

Detailed information about statistic data is described in the Viewing Workstation Statistics section.

The table below describes correspondence between flags in the **Statistics** tab of the **Server** settings and items of the control menu on the **Anti-virus network** page.

If you clear flags on the **Statistics** tab, corresponding items of the control menu become hidden.

Table 7-2. Correspondence between flags of Statistics data section and items of the control menu

Server parameters	Menu options
Quarantine state	General → Quarantine Configuration → Windows → Dr.Web Agent → Quarantine remote control flag
Hardware and software composition	General → Hardware and software General → Comparison of hardware and software
List of the station modules	Tables → Modules
List of installed components	General → Installed components
Sessions of stations users	General → Users sessions
Start/Stop of components	Tables → Start/Stop
Detected security threats	Tables → Threats Tables → Threat statistics
Scan errors	Tables → Errors
Scan statistics	Tables → Statistics Tables → Summary statistics
Agent installations	Tables → All network installations
Station tasks execution log	Tables → Tasks Tables → Virus Bases
Station statuses	Tables → Status Tables → Virus Bases
Virus database statuses	Tables → Virus Bases

7.2.4. Security

On the **Security** tab, you can configure restrictions for network addresses from which **Agents**, network installers and other ("neighboring") **Dr.Web Servers** will be able to access the **Server**.

To manage **Server** audit log, use the following flags:

- **Audit of administrator operations** allows to log operations of administrator with **Dr.Web Security Control Center** and writing the log into the DB.
- **Audit of server internal operations** allows to log **Dr.Web Server** internal operations and writing the log into the DB.
- **Audit of Web API operations** allows to log operations via XML API.

To view the audit log, select the **Administration** option in the main menu, then **Audit log** item in the control menu.

The **Security** tab contains additional tabs on which you can set the restrictions for the correspondent types of connections:

- **Agents** – the list of limitations on IP addresses from which **Dr.Web Agents** can connect to this **Server**.
- **Installations** – the list of limitations on IP addresses from which **Dr.Web Agents** installers can connect to this **Server**.
- **Neighbors** – the list of limitations on IP addresses from which neighbor **Dr.Web Servers** can connect to this **Server**.
- **Discovery service** – the list of limitations on IP addresses from which broadcast queries can be received by the Server Detection Service.

To set access restrictions for any type of connection:

1. Go to the correspondent tab (**Agents**, **Installations**, **Neighbors** or **Discovery service**).
2. To allow all connections, clear the **Use this ACL** flag.
3. To specify lists of allowed or denied addresses, set the **Use this ACL** flag.
4. To allow the access from a specific TCP address, include it into the **TCP: Allowed** or **TCPv6: Allowed** list.
5. To deny specific TCP address, include it into the **TCP: Denied** or **TCPv6: Denied** list.

To edit the address list:

1. Specify the address in the corresponding field and click **Save**.
2. To add a new field, click the button in the corresponding section.
3. To delete a field, click .

   The network address is specified as: *<IP-address>*/[*<prefix>*].

Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

Examples of prefix usage:

1. Prefix 24 stands for a network with a network mask: `255.255.255.0`

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`

2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16387064 addresses (256*256*256).

   Host addresses look like: `125.*.*.*`

The addresses not included into any of the lists are allowed or denied depending on whether the **Denial priority** flag is set. If the flag is set, the **Denied** list has a higher priority than the **Allowed** list. Addresses not included in any of the lists or included into both of them are denied. Allowed only addresses that are included in the **Allowed** list and not included in the **Denied** list.

7.2.5. Cache

On the **Cache** tab, you can configure the following parameters of **Server** cache cleanup:

- **Cache flush period** – period of full cache flush.
- **Quarantined files** – cleanup interval of quarantined files.
- **Installation packages** – cleanup interval of personal installation packages.
- **Repository files** – cleanup interval of files in repository.

When setting numerical values, please note the drop-down lists with unit of measure for intervals.

7.2.6. Database

On the **Database** tab, you can configure a DBMS required for **Dr.Web Server** operation.

You can get the structure of **Dr.Web Server** DB via the `init.sql` script, located in the `etc` subfolder of **Dr.Web Server** installation folder.

To specify parameters of operating with the Database:

1. On the **Database** tab of the **Dr.Web Server configuration** section, select the type of DB in the **Database** drop-down list:
   - **IntDB** – embedded SQLite2 DB (a component of **Dr.Web Server**),
   - **ODBC** – to use external DB via the ODBC connection,
   - **Oracle** – external DB for all platforms except FreeBSD,

If an **Oracle** external DBMS is used via the ODBC connection, it is necessary to install the latest version of the ODBC driver delivered with this DBMS. It is strongly recommended not to use the Oracle ODBC driver supplied by Microsoft.

   - **PostgreSQL** – external DB,
   - **SQLite3** – embedded DB (a component of **Dr.Web Server**). The recommended option when using an embedded database.
2. Specify requirement settings for DB operation:
   - For an embedded DB, if necessary, specify the full path to the database file into the **Path** field and specify the cache size and the data log mode.
   - The parameters of an external DB are described in detail in the **Appendices** document in Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver.
3. Click **Save** to apply specified settings.

Dr.Web Server distribution kit contains embedded clients for supported DBMS, so note:

- If you plan to use embedded DBMS clients which are supported within **Dr.Web Server**, then during installation (upgrade) of the **Server**, in the installer settings, select the **Custom** option of the installation and in the next window make sure that installation of corresponding embedded DBMS client is enabled in the **Database support** section.

- If you plan to connect external databases via ODBC, then during installation (upgrade) of the **Server**, in the installer settings, select the **Custom** option of the installation and in the next window disable the installation of corresponding embedded client in the **Database support** section.
  Otherwise, interaction with DB via ODBC will be impossible because of libraries conflict.

Server installer supports change mode of the product. To add or remove separate components e.g. databases management drivers, it is enough to run **Server** installer and select the **Change** option.

Using an embedded DBMS is selected by default. This mode considerably increases the load on the **Server**. It is recommended to use an external DBMS in large anti-virus networks. Changing the type of the DBMS is described in the **Appendices**, document, in the Changing the Type of the DBMS for Dr.Web Enterprise Security Suite section.

An embedded DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Dr.Web Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.

Otherwise, you must use an external DB.

If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:

- 3 GHz processor CPU,
- RAM at least 4 GB for **Dr.Web Server** and at least 8 GB for the DB server,
- UNIX system-based OS.

It is possible to perform transactions connected with clearing the database used by **Dr.Web Server**, in particular to delete records of events and data about the workstations which have not visited the **Server** for a certain period of time. To clear the database, open the Server schedule and add a corresponding task.

7.2.7. Proxy

On the **Proxy** tab, you can configure parameters of proxy server.

Set the **Use proxy server** flag to setup connections with **Dr.Web Server** via the proxy server. The following fields become available:

- **Proxy server** – IP address or DNS name of proxy server.
- To use authorization for access the proxy server according specified methods, set the **Use authorization** flag and specify the following parameters:
  - Specify the **Proxy server user** and **Password of proxy server user** fields.
  - Select one of authorization methods:

Option		Description
Any supported method		Use any authorization method supported by the proxy server. If the proxy server supports several authorization methods, the most secured is used.
Any safe supported method		Use any secured authorization method supported by the proxy server. In this mode, the Basic authorization method is not supported. If the proxy server supports several authorization methods, the most secured is used.
The following methods:	Basic authorization	Use Basic authorization. It is not recommended to use this method because transfer of authorization accounting data is not encrypted.
	Digest authorization	Use Digest authorization. Cryptographic authorization method.

Option		Description
	NTLM authorization	Use NTLM authorization. Cryptographic authorization method. The NTLM protocol of Microsoft company is used for authorization.
	GSS-Negotiate authorization	Use GSS-Negotiate authorization. Cryptographic authorization method.

7.2.8. Transport

On the **Transports** tab, you can configure parameters of transport protocols used by the **Server** to connect with clients.

In the **TCP/IP** subsection, parameters of connection with the **Server** via TCP/IP are set:

- **Address** and **Port** – correspondingly the IP address and the port number of the network interface to which this transport protocol is bound. **Server** listens interface with specified parameters to communicate with **Agents** that installed on workstations.
- **Name** – the name of **Dr.Web Server**. If no name is specified, the name set on the **General** tab is used (see above, if no name is set on the tab, the computer name is used). If the other name specified for the protocol than the name from the **General** tab, the name from the protocol description is used. This name is used by detection service to find **Server** by **Agents** and etc.
- Set the **Discovery** flag to enable **Server** discovery service.
- Set the **Multicasting** flag to use the *Multicast over UDP* mode for detecting the **Server**.
- **Multicast group** – IP address of multicast group in which the **Server** is registered. It is used for communication of **Agents** and **Network installers** when searching active **Dr.Web Servers** in the network. If field is not specified, the `231.0.0.1` group is used by default.
- Under UNIX system-based OS only: in the **Path** field, specify the path to the connection socket, e.g., with the **Agent**.

See the Setting the Network Connections section for more details.

This parameters should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

7.2.9. Modules

On the **Modules** tab, you can configure protocols for interaction of the **Server** with other **Dr.Web Enterprise Security Suite** components.

- Set the **Dr.Web Security Control Center extension** flag to use **Dr.Web Security Control Center Extension** for managing the **Server** and anti-virus network via the **Control Center**,

If you clear the **Dr.Web Security Control Center extension** flag, when after reboot of **Dr.Web Server**, **Dr.Web Security Control Center** will be not available. You will be able to manage the **Server** and anti-virus network only via the remote diagnostics utility, if the **Dr.Web Server FrontDoor extension** flag is set.

- Set the **Dr.Web Server FrontDoor extension** flag to use **Dr.Web Server FrontDoor** extension that allows connections of **Server** remote diagnostics utility (see also Dr.Web Server Remote Access).
- Set the **Dr.Web Agent protocol** flag to enable protocol that allows interaction of the **Server** with **Dr.Web Agents**.

- Set the **Microsoft NAP Health Validator protocol** to enable protocol that allows interaction of the **Server** with the Microsoft **NAP Validator** component of system health validating.
- Set the **Dr.Web Agent installer protocol** flag to enable protocol that allows interaction of the **Server** with **Dr.Web Agent** installers.
- Set the **Dr.Web Servers cluster protocol** flag to enable protocol for interaction between **Servers** in the cluster system.
- Set the **Dr.Web Server protocol** flag to enable protocol that allows interaction of **Dr.Web Server** with other **Dr.Web Servers**. The protocol is disabled by default. If you use multi-server network configuration (see Peculiarities of a Network with Several Dr.Web Servers), set the **Dr.Web Server protocol** flag to enable this protocol.

7.2.10. Cluster

On the **Cluster** tab, you can configure parameters of **Dr.Web Servers** cluster for data exchange in multiserver anti-virus network configuration.

To use the cluster, specify the following parameters:

- **Multicast group** – IP address of multicast group through which **Servers** will be exchange information.
- **Port** – port number of network interface to which transport protocol is bound to transmit the information into multicast group.
- **Interface** – IP address of network interface to which transport protocol is bound to transmit the information into multicast group.

Peculiarities of **Dr.Web Server** clustering are given in the Dr.Web Servers Cluster section.

7.2.11. Location

On the **Location** tab, you can specify additional information about the physical location of the computer on which **Dr.Web Server** is installed.

Also on this tab you can view the **Server** location on a geographical map.

To view the Server location on a map:

1. In the **Latitude** and **Longitude** fields, specify the **Server** geographical coordinates in the Decimal Degrees format.
2. Click **Save** to save specified data to the **Server** configuration file.

   To view the map, you do not need to restart the **Server**. But to apply changed geographical coordinates, you must restart the **Server**.
3. On the **Location** tab, the OpenStreetMaps preview will be shown containing a mark according to the specified coordinates.

   If the preview cannot be loaded, the **Show on map** text displays.
4. To view the full size map, click the preview or the **Show on map** text.

7.2.12. Download

On the **Download** tab, you can configure **Server** parameters for generating **Agent** installation files for an anti-virus network stations. Further these parameters are used for connecting **Agent** installer to the **Server**:

- **Dr.Web Server address** – IP address or DNS name of **Dr.Web Server**.

  If **Server** address is not specified, computer name returned by the operating system is used.

- **Port** – port number which is used for connecting **Agent** installer to the **Server**.

  If the port number is not specified, the 2193 port is used (it is configured in the **Control Center**, at **Administration** → **Dr.Web Server configuration** → the **Transport** tab).

The settings of the **Download** section are saved in the `download.conf` confiduration file (see the **Appendices** document, p. G3. Download.conf Configuration File).

7.2.13. Multicast Updates

On the **Multicast updates** tab, you can configure updates transmission on workstations via the multicast protocol.

Set the **Enable multicast updates** flag to enable transmission of updates to stations via the multicast protocol, in so doing:

- If multicast updates are disabled, updating of all stations is performed only in general mode - via the TCP protocol.
- If multicast updates are enabled, when for all stations connected to this **Server** updating is performed in two stages:
  1. Update via multicast protocol.
  2. General update via the TCP protocol.

To setup multicast updates, use the following parameters:

- **UDP datagram size (bytes)** – size of UDP datagrams in bytes.

  Allowed range is 512 - 8192. To avoid fragmentation, it is recommended to set a value less than MTU (Maximum Transmission Unit) of the network.

- **File transmission time (ms.)** – during specified time, single update file is transmitted, after that **Server** starts sending the next file.

  All files which failed to transmit at the step of multicast protocol update, will be transmitted at standard update process over the TCP protocol.

- **Multicast updates duration (ms.)** – duration of update process via multicast protocol.

  All files that failed to transmit during update stage via multicast protocol will be transmitted in process of standard update via TCP protocol.

- **Packages transmission interval (ms.)** – interval of packages transmission to a multicast group.

  The low interval value may cause significant losses during package transfer and network overload. It is not recommended to change this parameter.

- **Interval between retransmission requests (ms.)** – with this interval **Agents** send requests for retransmission of lost packages.

  Server accumulates these requests after that sends lost blocks.

- **"Silence" interval on the line (ms.)** – when a file transmission is over before allowed time has expired, if during specified "silence" interval no requests from **Agents** for retransmission of lost packages are received, **Server** considers that all **Agent** received updates files and starts sending the next file.
- **Retransmission requests accumulation interval (ms.)** – during specified interval, **Server** accumulates requests from **Agents** for retransmission of lost packages.

  Agent request lost packages. **Server** accumulates these requests during specified time slot after that sends lost blocks.

To specify the list of multicast groups from which multicast updates is available, setup the following parameters in the **Multicast groups** section:

- **Multicast group** – IP address of multicast group in which stations receive multicast updates.
- **Port** – port number of **Dr.Web Server** network interface, to which transport multicast protocol is bound for updates transmission.

For multicast updates, you must specify any unused port, particularly, different from the port that is specified in the settings of transport protocol for **Server** operating.

- **Interface** – IP address of **Dr.Web Server** network interface, to which transport multicast protocol is bound for updates transmission.

  Every line contains setup of one multicast group. To add one more multicast group, click .

When you configure several multicast groups, please note the following features:

- For different **Dr.Web Servers**, which will distribute multicast updates, must be different multicast groups specified.
- For different **Dr.Web Servers**, which will distribute multicast updates, must be different **Interface** and **Port** parameters specified.
- For using several multicast groups, sets of stations which are included into these groups must not overlap. Thus, each station of anti-virus network can be included only into one multicast group.

7.2.14. Licenses

On the **Licenses** tab, you can configure settings of licenses propagation between **Dr.Web Servers**:

- **Validity period of donated licenses** – time period on which licenses are donated from the key on this **Server**. The setting is used if the **Server** donates licenses to neighbor Servers.
- **Period for accepted licenses renewal** – period till the license expiration, starting from which this **Server** initiates renewal of the license which is accepted from the neighbor **Server**. The setting is used if the Server accepts licenses from neighbor **Servers**.
- **License synchronization period** – interval for synchronizing information about donating licenses between **Servers**.

Detailed information on licenses propagation between **Servers** is described in the License Manager section.

7.3. Dr.Web Server Remote Access

For connection of the **Server** remote diagnostics utility, you must enable **Dr.Web Server FrontDoor** extension. To do this, in the **Dr.Web Server configuration** section, on the Modules tab, set the **Dr.Web Server FrontDoor extension** flag.

For connection of the **Server** remote diagnostics utility, administrator that connects via the utility, must have the **Use additional features** permission. Otherwise, access to the **Server** via the remote diagnostics utility will be forbidden.

To configure parameters for Server remote diagnostics utility:

1. Select the **Administrating** item in the main menu of the **Control Center**, in the opened window, select **Dr.Web Server remote access** in the control menu.
2. Specify the following parameters:
   - **SSL certificate** – SSL certificate file which will be verified on connection. The drop-down list contains available certificates from the **Server** folder.
   - **SSL private key** – SSL private key file which will be verified on connection. The drop-down list contains available private keys from the **Server** folder.
   - **Address** – address from which the **Server** remote diagnostics utility can be connected.
   - **Port** – port to connect the **Server** remote diagnostics utility. The 10101 port is used by default.
3. Click **Save**.

You can view the usage description of the console version of the **Server** remote diagnostics utility in the **Appendices** document, p. H9. Dr.Web Server Remote Diagnostics Utility.

7.4. Setting Dr.Web Server Schedule

To edit Dr.Web Server schedule, perform the following actions:

1. Select the **Administrating** item in the main menu of the **Control Center**, in the opened window, select **Dr.Web Server Task Scheduler** in the control menu. The list with the **Server** tasks will be opened.
2. To manage schedule, use the corresponding elements from the toolbar:

   a) General elements on the toolbar are used to create new tasks and generally manage schedule section. These tools are always available on the toolbar.

   Create task – add a new task. This action is described in details below, in the Task Editor section.

   Export settings from this section to the file – export schedule to the file of special format.

   Import settings to this section from the file – import schedule from the file of special format.

   b) To manage existing tasks, set the flags next to the necessary tasks or the common flag in the table header to select all task from the list. At this, elements on the toolbar to manage selected tasks become available.

Table 7-3. Toolbar elements for managing selected tasks

Option		Action
Status	**Enable execution**	Activate execution of selected tasks according to their schedule, if they were disabled.

Option		Action
	Disable execution	Disable execution of selected tasks. Tasks remain on the list but will not be executed.
The same action you can perform from the task editor on the **General** tab by setting the **Enable execution** flag.		
Severity	**Make critical**	Perform extra launch of the task at next **Dr.Web Server** launch, if scheduled execution of this task has been omitted.
	Make not critical	Execute the task only at scheduled time regardless of whether a task launch has been omitted or not.
The same action you can perform from the task editor on the **General** tab by setting the **Critical task** flag.		
Duplicate settings		Duplicate tasks that are selected in the list of current schedule. When you run the **Duplicate settings** option, new tasks are created with settings similarly to the selected tasks.
Schedule repeatedly		For tasks which executed once: execute task one more time according to the specified time settings (changing execution multiplicity of the task is described below, in the Task Editor section).
Remove these settings		Remove selected task from the schedule.

3. To change task parameters, select it in the tasks list. The **Task editor** window described below opens.
4. After editing the schedule, click **Save** to accept changes.

Task Editor

In the **Task Editor** you can specify settings to:

1. Create a new task.

   For this click **Create task** on the toolbar.

2. Edit existing task.

   For this click the name of one of the tasks in the tasks list.

The window for editing a task opens. Settings for editing of existing task are similar to the settings of creating a new task.

Values of fields, marked with the * sign, must be obligatory specified.

To edit task settings:

1. On the **General** tab you can setup the following parameters:
   - In the **Name** field, specify the name of the task displayed in the schedule list.
   - To enable the task execution, set the **Enable execution** flag. If the flag is cleared, the task remains on the list but will not be executed.

The same action you can perform from the main window of the schedule via the **Status** option on the toolbar.

- The **Critical task** flag instructs to perform extra launch of the task at next **Dr.Web Agent** launch, if scheduled execution of this task has been omitted (**Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after **Dr.Web Agent** has been launched.

The same action you can perform from the main window of the schedule via the **Severity** option on the toolbar.

2. On the **Action** tab, in the **Action** drop-down list, select the type of the task and specify task parameters which are needed to perform the task.

Table 7-4. Tasks types and their parameters

Task type	Parameters and description
Back up critical server data	The task is designed to backup the following critical data of the **Server**: • database, • license key file, • private encryption key. Specify the following parameters: • **Path -** path to the directory where the data will be saved (blank field means that the default directory will be used). • **Maximum number of copies –** maximum number of backup copies (the 0 value means no limitation). For details see the **Appendices** document, p. Appendix H5.5.

Back up repository	The task is designed for periodic backups of the repository.
	Specify the following parameters:
	• **Path** - full path of the directory where the backup copy will be stored.
	• **Maximum number of copies** - maximum number of repository backup copies which are stored by the task in the specified directory. If the maximum number of copies is reached, the oldest copy will be overwritten by the new one.
	• **Repository area** defines which part of information on anti-virus component will be saved:
	  ○ **Entire repository** - save all revisions from the repository for the components that are selected in the list below.
	  ○ **Only critical revisions** - only revisions marked as important will be saved for the components that are selected in the list below.
	  ○ **Only configuration files** - only configuration files will be saved for the components that are selected in the list below.
	• Set the flags for the components selected areas of which will be saved.

Create statistic report	The task is designed to create a report with statistics on the anti-virus network. To be able to create a report it is mandatory to enable the **Periodic report** notification (see Notification Configuration). The generated report is saved on a computer where the **Server** is installed. Report delivery depends on the type of notification: • For sending messages via **Email**: a letter with attached report and also the link to the report location is sent to the mail address which is specified in notification settings. • For all other methods of delivery: an appropriate notification with a link to the report location is sent. To create a task in the schedule you have to specify the following parameters:

Task type	Parameters and description
	• **Notifications profiles** - name of notifications group with common settings for report generation. The title name can be specified when creating a new notifications group. • **Report language** - language of the data in the report. • **Date format** - format for dates display in statistic data. The following formats are available: o European: `DD-MM-YYYY HH:MM:SS` o American: `MM/DD/YYYY HH:MM:SS` • **Report format** - document format to save the statistics report. • **Report period** - time period for which the statistics will be included in the report. • **Groups** - list of anti-virus network station groups which data will be included in the report. To select multiple groups, use the CTRL or SHIFT. • **Report tables** - list of statistical tables which data will be included in the report. To select multiple tables, use the CTRL or SHIFT. • **Report retention period** - time period for storing a report on the computer with running **Server**, starting from report generation.
Execute hook	The task is designed for executing user hooks (see the User Hooks section). In the **Name** drop-down list, select a group of user hooks that will be executed.
Execute script	The task is designed for executing Lua script which is specified in the **Script** field.
License expiration reminder	The task is designed to issue reminders about the license expiration of **Dr.Web** product. You have to set the period preceding license expiration starting from which the reminders will be issuing.
Neighbor server has not connected for a long time	The task is designed to issue notifications in case the neighbor **Servers** have not been connected to the current **Server** for a long time. Notifications display settings can be configured in the Notification Configuration section using the **Neighbor server has not been connected for a long time** item. Set values in the **Hours** and **Minutes** fields to define a time period after which the neighbor **Server** will be considered as not connected for a long time.
Purge database	The task is designed to collect and purge unused records in the **Server** database using the `vacuum` command. No additional parameters required to run the task.
Purge old records	The task is designed to purge outdated information about the stations from the database. You have to specify the number of days after which the statistic records on workstations (but not the workstations themselves) are considered outdated and purged from the **Server**. The period after which the statistic records are purged is specifies for each type of records separately.
Purge old stations	The task is designed to purge outdated stations from the database. You have to specify the time period (90 days by default) after which all stations that did not have at least one connection to the **Server** are considered old and are purged from the **Server**.
Purge outdated messages	The task is designed for purging the following messages from the database: • agent notifications, • notifications for the web console, • reports created according to the schedule.

Task type	Parameters and description
	This also purges messages marked as obsolete, i.e. with expired retention period which can be configured: • for notifications: for appropriate sending method while creating a notification (see Notification Configuration). • for reports: in a task for creating reports. No additional parameters required to run the task.
Purge unsent events	The task is designed to purge unsent events from the database. You have to set the period for storing unsent events after which they will be purged. This refers to events that a subordinate **Server** sends to a master **Server**. If sending a message fails, it is moved to the unsent messages list. A subordinate **Server** continues its attempts to send the message at the specified interval. When the **Purge unsent events** task is run, events will be purged if their storage time has reached and exceeded specified period.
Replace encryption key	The task is designed for periodic replacement of the following encryption keys: • the `drwcsd.pri` private key on the **Server**, • the `drwcsd.pub` public key on workstations. Because some workstations can be turned off at the time of replacement, the procedure is divided into two steps. You have to create two tasks to perform each of these steps, it is recommended to perform the second step some time after the first one, when certain stations will probably connect to the **Server**. When creating a task, select the appropriate step of key replacing from the drop down list: • **Adding a new key** - the first step of the procedure when the new inactive encryption key pair is created. The stations get the new public key upon the connection to the **Server**. • **Deleting the old key and switching to the new key** - the second step when the stations are notified about switching to the new encryption keys, followed by replacing the existing keys with the new ones: public keys on the stations and private key on the **Server**. If for any reason some stations did not receive the new public key, they will not be able to connect to the **Server**. To resolve this problem, the following options are available: • Manually put the new public key on the station (you can view the procedure of replacing the key on station, in the **Appendices** document, p. Connecting Dr.Web Agent to Other Dr.Web Server). • Allow the **Agents** authorize on the **Server** with incorrect public key (see the Network section in the **Agent** preferences).
Restart Dr.Web Server	The task is designed to restart the **Server**. No additional parameters required to run the task.
Run program	The task is designed to run custom program. Specify the following parameters: • The **Path** field **-** full name (with the path) of the program executable file to run. • The **Arguments** field **-** command line parameters to run the program. • Set the **Run synchronously** flag for the synchronization with **Server** – wait while task finishes before executing other tasks with **Run program** type. If the **Execute synchronously** flag is cleared, the **Server** logging only the start of the program. If the **Execute synchronously** flag is set, the **Server** logging the start of the program, the returned code and the time of the program end.
Send message to station	The task is designed to send arbitrary message to users of a station or group of stations.

Task type	Parameters and description
	A message settings are given in the Sending Notifications to Users section.
Shut down Dr.Web Server	The task is designed to shut down the **Server**. No additional parameters required to run the task.
Station has not connected for a long time	The task is designed to issue notifications in case the stations have not been connected to the current **Server** for a long time. Notifications display settings can be configured in the Notification Configuration section using the **Station has not been connected for a long time** item. In the **Days** field specify a time period after which the station will be considered as not connected for a long time.
Synchronization with Active Directory	The task is designed to synchronize network structures: Active Directory containers which contains computers become groups of anti-virus network to which workstations are placed. No additional parameters required to run the task. The task is disabled by default. To activate the task execution, set the **Enable execution** option in the task settings or on the toolbar as described above.
Update repository	The information on this task can be found in the Scheduled Updates section.
Wake stations	The task is designed to turn on stations, for example before running the scanning task. The following task parameters define which stations will be turned on: • **Wake all stations** - every station which is connected to the **Server** will be turned on. • **Wake stations by specified parameters** - only stations that accord to the parameters below will be turned on: ○ **IP addresses** - the list of IP addresses of the stations that will be turned on. The list is specified in the following format: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Use comma or newline to separate several addresses. You can also use DNS names of the stations instead of their IP addresses. ○ **MAC addresses** - the list of MAC addresses of the stations that will be turned on. The MAC-address octets have to be separated by the ':' sign. Use comma or newline to separate several addresses. ○ **Group identifiers** - the list of group identifiers of the stations that will be turned on. Use separate field for each new identifier. Click to add a new field. To remove the identifier click next to it. To run this task, all stations that are going to be turned on should be equipped with network cards with Wake-on-LAN support. To check whether your network card supports Wake-on-LAN, please refer to its documentation or see its properties (**Control Panel → Network and Internet → Network Connections → Change Adapter Settings → Configure → Advanced**).
Write to log file	The task is designed to write to the **Server** log file specified string. **String** - message to be logged.

Outdated information is purged from the database to save disc space. The period in the **Purge old records** and **Purge old stations** tasks by default is 90 days. If you decrease the value, the statistics on the operation of the anti-virus network components will be less representative. If you decrease the value, the **Server** may need extremely more resources.

Simultaneous execution of tasks with **Execute script** type on several **Servers** which use one database may result in errors.

3. On the **Time** tab:
   - In the **Period** drop-down list, set the launch mode of the task and setup the time according to the specified periodicity.

Table 7-5. Parameters of different launch modes

Launch type	Description
Daily	Specify the hour and the minute for the task to be launched at the time specified.
Every N minutes	The **N** value should be specified to set the time interval for the execution of the task. At **N** equal 60 or more, the task will be run every **N** minutes. At **N** less than 60, the task will be run every minute of the hour multiple of **N**.
Hourly	Specify a number from 0 to 59 to set the minute of every hour the task will be run.
Monthly	Specify the day of the month, the hour and the minute for the task to be launched at the time specified.
N minutes after initial task	In the **Initial task** drop-down list, select the task relatively to which the time of current task execution is set. In the **Minute** field, specify or select from the offered list the number of minutes that should pass after the execution of initial task to start execution of edited task.
Shut down	The task will be launched at **Server** shut down. No additional parameters required to run the task.
Start up	The task will be launched at **Server** start up. No additional parameters required to run the task.
Weekly	Select a day of the week, specify the hour and the minute, for the task to be launched at the time specified.

   - Set the **Disable after the first execution** flag to execute the task only once at specified time. If the flag is cleared, the task will be executed multiple times according to the specified periodicity.

   To repeat the launch of task already ones executed, use the **Schedule repeatedly** on the toolbar of the schedule section.
4. When all parameters for the task are specified, click **Save** to accept changes of edited parameters, if you editing existing task, or to create a new task with specified parameters if you created a new task.

7.5. Setting the Web Server Configuration

To set the configuration parameters of the Web server:

1. Select the **Administration** item in the main menu of the **Control Center**.
2. Select **Web server Configuration** in the control menu. A window with **Web server** configuration will be opened.

Values of fields, marked by the * sign, must be obligatory specified.

3. On the toolbar, the following buttons to manage the section settings are available:

   Restart Dr.Web Server – restart the **Server** to apply changes that have been specified in this section. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Restore configuration from the backup – drop-down list with the backup of all section settings, which you can restore after making changes. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Reset all parameters to initial values – restore the values that all parameters in this section had before current editing (last saved values).

   Reset all parameters to default values – restore default values of all parameters in this section.
4. To apply the changes specified in the section settings, click **Save**, after this the **Server** must be rebooted. To do this, click **Restart Dr.Web Server** on the toolbar of this section.

7.5.1. General

On the **General** tab, specify the following **Web server** settings:

- **Dr.Web Server address** – IP address or DNS name of **Dr.Web Server**.

  Parameter is specified in the following format:

  <Server IP address or DNS name>`[:`*<port>*`]`

  If the **Server** address is not specified, computer name returned by the operating system or the **Server** network address: DNS name, if available, otherwise - IP address are used.

  If the port number is not specified, the port from a request is used (e.g., for requests to the **Server** from the **Control Center** or via the **Web API**). Particularly, for the requests from the **Control Center** it is the port specified in the address line for connection of the **Control Center** to the **Server**.

  The value is stored in the `<server-name />` parameter of the `webmin.conf` configuration file.

  This parameter value is also used to generate the link for downloading the **Agent** installation file for an anti-virus network stations.
- **Parallel requests number** – number of parallel requests processed by the **Web server**. This parameter affects server performance. It is not recommended to change this parameter without need.
- **IO threads number** – number of threads serving data transmitted in network. This parameter affects **Server** performance. It is not recommended to change this parameter without need.

- **Timeout (sec)** – HTTP session timeout. For persistent connections, **Server** releases the connection, if there are no requests received from a client during specific time slot.
- **Minimal send rate (BPS)** – minimal acceptable data send rate. If outgoing network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.
- **Minimal receive rate (BPS)** – minimal acceptable data receive rate. If incoming network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.
- **Send buffer size (KB)** – size of buffers used when sending data. This parameter affects server performance. It is not recommended to change this parameter without need.
- **Receive buffer size (KB)** – size of buffers used when receiving data. This parameter affects server performance. It is not recommended to change this parameter without need.
- **Max request length (KB)** – Maximum allowed size of HTTP request.
- **Use compression** – set the flag to use traffic compression for data transmission over a communication channel with the **Web server** via HTTP/HTTPS.
  - If the flag is set, the **Compression level** drop-down list become available. In this list, you can select the data compression level from 1 to 9, where the 1 is minimal level and the 9 is maximal compression level.
- **Replace IP addresses** – set the flag to replace IP address with DNS names of computers in the **Server** log file.
- **Keep-alive SSL connection** – set the flag to use keep-alive SSL connection. Older browsers may not work properly with regular SSL connections. Disable this parameter, if you have problems with SSL protocol.
- **SSL certificate** – path to SSL certificate file. The drop-down list contains available certificates from the **Server** folder.
- **SSL private key** – path to SSL private key file. The drop-down list contains available private keys from the **Server** folder.

7.5.2. Additional

On the **Additional** tab, specify the following **Web server** settings:

- Set the **Show script errors** flag to show script errors in browser. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.
- Set the **Trace scripts** flag to enable scripts tracing. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.
- Set the **Abort scripts** flag to allow aborting of scripts execution. This parameter is used by technical support and developers. It is not recommended to change this parameter without need.

7.5.3. Transport

On the **Transport** tab, you can configure network addresses to listen for accepting incoming connections by the **Web server**, e.g., for connection of the **Control Center** or executing requests via the Web API:

- In the **Addresses to listen on HTTP** section, you can configure the list of interfaces to listen for accepting connections via the HTTP protocol:

  In the **Address** and **Port** fields, specify correspondingly the IP address and the port number of the network interface from which HTTP connections can be accepted.

  By default, the following parameters are set to "listen" by the **Web server**:

  - **Address**: `0.0.0.0` – use "all network interfaces" for this computer, on which the **Web server** is installed.
  - **Port**: `9080` – use the standard `9080` port for the HTTP protocol.

- In the **Addresses to listen on HTTPS** section, you can configure the list of interfaces to listen for accepting connections via the HTTPS protocol:

  In the **Address** and **Port** fields, specify correspondingly the IP address and the port number of the network interface from which HTTPS connections can be accepted.

  By default, the following parameters are set to "listen" by the **Web server**:

  - **Address**: `0.0.0.0` – use "all network interfaces" for this computer, on which the **Web server** is installed.
  - **Port**: `9081` – use the standard `9081` port for the HTTPS protocol.

To add a new address field, click in the corresponding section. To delete a field, click next to the deleting field.

7.5.4. Security

On the **Security** tab, you can configure restrictions for network addresses from which the **Web server** receives HTTP and HTTPS requests.

To setup access limitations for any of connection type:

1. To allow the access by HTTP or by HTTPS from definite addresses, add them to the **HTTP: Allowed** or **HTTPS: Allowed** lists correspondingly.
2. To deny the access by HTTP or by HTTPS from definite addresses, add them to the **HTTP: Denied** or **HTTPS: Denied** lists correspondingly.
3. The addresses not included into any of the lists are allowed or denied depending on whether the **HTTP denial priority** and **HTTPS denial priority** flags are set: if the flag is set, the addresses not included into any of the lists (or included into both of them) are denied. Otherwise, such addresses are allowed.

To edit the address list:

1. Specify the network address in the corresponding field and click **Save**.
2. To add a new field, click in the corresponding section.
3. To delete a field, click .

   The network address is specified as: *<IP-address>*`/[`*<prefix>*`]`.

Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

Examples of prefix usage:

1. Prefix 24 stands for a network with a network mask: `255.255.255.0`

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`

2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16387064 addresses (256*256*256).

   Host addresses look like: `125.*.*.*`

7.6. User Hooks

User hooks, implemented as a lua-scripts, are meant for automation of the administrator work enabling quicker performance of certain tasks of **Dr.Web Server**.

User hooks are located in the following subfolder of the **Server** installation folder:

- for Windows OS: `var\extensions`
- for FreeBSD OS: `/var/drwcs/extensions`
- for Linux OS and Solaris OS: `/var/opt/drwcs/extensions`

After the **Server** installation, preinstalled user hooks are located in this folder.

It is recommended to edit user hooks via the **Control Center**.

To configure user hooks execution:

1. Select the **Administration** item in the main menu of the **Control Center**.
2. In the opened window, select the **User hooks** item in the control menu. User hooks settings window will be opened.

Hooks Tree

Hooks hierarchical list displays the tree view, nodes of which are hook groups and user hooks included into them.

Initially, hooks tree contains the following preinstalled groups:

- **Examples of the hooks** – contains templates of all available user hooks. On the base of these templates you can create your own user hooks.
- **IBM Tivoli integration** – contains templates of user hooks used in integration with IBM Tivoli system.

The icon of the tree element depends on the type and status of this element (see table 7-10).

Table 7-10. Icons of elements in the hooks tree

Icon	Description
Hooks groups	
	Hooks group for which hook execution is enabled.
	Hooks group for which hook execution is disabled.
Hooks	
	Hook which is enabled to execute.
	Hook which is disabled to execute.

Hooks Tree Managing

To manage objects in the hooks tree, use the following elements of the toolbar:

– drop-down list for adding an element to the hooks tree:

Add hook – add a new user hook.

Add hooks group – add a new user group for placing hooks in it.

Remove selected objects – remove user hook or hooks group which is selected in the hook tree.

Enable hook execution – the same action is performed in the hooks editor if you set the **Enable hook execution** flag. See also Hooks activating.

Disable hook execution – the same action is performed in the hooks editor if you clear the **Enable hook execution** flag. See also Hooks activating.

Hooks Groups Managing

To create a new group:

1. On the toolbar, select > **Add hooks group**.
2. In the opened window, specify the following parameters:
   - Set the **Enable hook execution** flag to activate hooks which will be included into this group. See also Hooks activating.
   - In the **Group name** field, specify an arbitrary name for the creating group.
3. Click **Save**.

To change the order of groups using:

1. In the hooks tree, drag and drop the hooks group and place it in the necessary order relative to the other groups.
2. The order of hooks usage is automatically changed after changing groups order: the first will be performed the hooks from the groups that are placed higher in the hooks tree.

To move a hook to the other group:

1. In the hooks tree, select a hook you want to move.
2. On the opened properties pane, in the **Parent group** drop-down list, select the group into which you want to move the hook.
3. Click **Save**.

Hooks Managing

To create a new hook:

1. On the toolbar, select > **Add hook**.
2. In the opened window, specify the following parameters:
   - Set the **Enable hook execution** flag to activate the creating hook. See also Hooks activating.
   - In the **Parent group** drop-down list, select the group into which you want to place the creating hook. Further, you can move the hook into other group - see above.
   - In the **Hook** drop-down list, select the hook type. The hook type defines an action for which the hook will be called.
   - In the **Hook text** field, enter the lua script which will be executed when the hook called.
     The **Information on hook** subsection contains an action for which the hook will be called; information whether the **Server** database is available or not for this hook; and also contains the lists of input parameters and returned values for this type of hook.
3. Click **Save**.

To edit a hook:

1. In the hooks tree, select a hook you want to edit.
2. In the right part of the window, the properties pane for this procedure automatically opens. You can edit all parameters which are specified on creating the hook except the **Hook** parameter. This parameter defines an action for which the hook will be called, and cannot be edited after the hook has been created.

3. Click **Save**.

Hooks Activation

Activation of hooks and hooks groups defines whether the hooks will be executed on corresponding event or not.

To activate a hook or a group of hooks:

1. In the hooks tree, select a hook or a hooks group you want to activate.
2. Perform one of the following actions:
   - On the toolbar, click **Enable hook execution**.
   - In the right part of the window on the properties pane of the selected object, set the **Enable hook execution** flag if it is cleared. Click **Save**.

Hooks activation features:

To execute a hook on corresponding event, the following is necessary:

a) the hook itself must be activated;
b) the group wich contains the hook must be activated.

If a hooks group is disabled, its hooks will not be executed even if they are activated.

On group activating, only whose hooks will be executed that are directly activated.

7.7. Setting Notifications

Dr.Web Enterprise Security Suite allows to send notifications about virus attacks, anti-virus network components states and other events to administrators of **Dr.Web Enterprise Security Suite** anti-virus network.

7.7.1. Notification Configuration

To configure notifications on anti-virus network events:

1. Select the **Administration** item in the main menu of the **Control Center**. In the opened window, select **Notifications configuration** in the control menu.
2. At initial setup, notifications list is empty. Click **Add notification**.
3. To enable notifications sending, set the switch on the left of the notifications block header to the corresponding position:

   – notifications sending for this block is enabled.

   – notifications of this block are not sent.
4. In this section, you can create several notifications blocks (profiles), e.g., for the different sending methods. To add one more block, click on the right of the notifications block settings. At the bottom of the page, one more notifications block will be added. Configuration of different notifications blocks as their templates texts is performed independently.
5. In the **Title** field, specify the name of added notifications block. This name is used, e.g. in configuration of the **Statistic reports** in the **Server** schedule. Further, to edit the header, click it and type necessary name. If you have more than one notification blocks, when you click the header text, the drop-down list with headers of existing notifications blocks will be prompted.

6. To configure notifications sending, select necessary type for notifications sending from the **Notifications send method** drop-down list:
   - Dr.Web Agent – send notifications via the **Agent** protocol.
   - Email – send notifications on email.
   - Push-notifications – send push notifications to **Dr.Web Mobile Control Center**. This option is available in the **Notifications send method** drop-down list only after **Dr.Web Mobile Control Center** has been connected to this **Dr.Web Server**.
   - SNMP – send notifications via the SNMP protocol.
   - Web console – send notifications for viewing in the Web console.
   - Windows Message – send notifications using **Windows Messenger** (for **Servers** under Windows OS only).

   Settings description for each type of notifications sending is given in this section below.
7. For notifications sending, the predefined set of standard **Server** notifications is provided.

Description of predefined notifications and their parameters is given in the **Appendices** document, in p. Appendix D1. Predefined Notifications Description.

To configure concrete notification, do the following:

a) In the notifications list, set the flags next to those notifications that will be sent according to the send method of current notifications block.

b) To change notifications settings, click ⚙ next to the edited notification. Notification template will be opened. If necessary, edit the text of notification to send. In the notification text you can use template variables (in braces). To add variables, use drop-down lists on the message header. When a message is being generated, the system replaces template variables with a certain text, which depends upon its current parameters. The list of available variables is given in the **Appendices** document, in p. Appendix D3. The Parameters of the Notification System Templates.

c) For notifications from the **Station** subsection, you can set the list of stations on the events on which notifications will be send. In the template editing window, in the **Groups of monitored stations** tree, select groups of stations to monitor events and send corresponding notifications. To select several groups, use CTRL or SHIFT.

For the **SNMP** send method, notification template texts are set at the SNMP client side. Via the **Control Center** in the **Station** subsection, you can specify only the list of stations on the events on which notifications will be send.

8. After editing, click **Save** to apply all changes specified.

Notifications via the Agent Protocol

For notifications via the **Agent** protocol, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- **Station** – identifier of a station to which notifications must be send. You can view station identifier in the stations properties.
- **Notification storing time** – time period for storing a notification starting from its receiving. 1 day is by default. After specified period, notification is marked as outdated and deleted according to the **Purge outdated messages** task in the **Server** schedule settings.
- **Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

Notifications on Email

For notifications on email, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- **Sender email address** – email address of notifications sender.
- **Recipient email addresses** – email addresses of notifications receivers. Only one email address of a receiver per each field. To add one more receiver field, click . To remove the field, click .
- In the **SMTP server settings** section, specify the following parameters:
  - **Address** – SMTP server address which is used to send emails.
  - **Port** – SMTP server port which is used to send emails.
  - **User**, **Password** (**Retype password**) – if necessary, specify name and password of SMTP server user, if the SMTP server requires authorization.
  - Set the **STARTTLS encoding** flag to use *STARTTLS* traffic encoding for sending notification on email.
  - Set the **SSL encoding** flag to use *SSL* traffic encoding for sending notification on email.
  - Set the **Use CRAM-MD5 authentication** flag to use *CRAM-MD5* authentication on a mail server.
  - Set the **Use DIGEST-MD5 authentication** flag to use *DIGEST-MD5* authentication on a mail server.
  - Set the **Use the plain authentication** flag to use *plain text* authentication on a mail server.
  - Set the **Use LOGIN authentication** flag to use *LOGIN* authentication on a mail server.
  - Set the **Validate the SSL server certificate** flag to enable validating the SSL certificate of a mail server.
  - Set the **Debug mode** flag to get SMTP session detailed log.**Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

Push Notifications

For Push notifications which are sent to **Mobile Control Center**, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- **Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

Notifications via the SNMP Protocol

For notifications via the SNMP protocol, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- **Receiver** – entity that receives SNMP request. For example, IP address or DNS name. Only one receiver per each field. To add one more receiver field, click . To remove the field, click .

- **Sender** – entity that sends SNMP request. Defaults are: "localhost" for Windows and "" for UNIX.
- **Community** – SNMP community or context. Default is public.
- **Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

Notifications Displayed in the Web Console

For notifications displayed in the **Web console**, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- **Notification storing time** – time period for storing a notification starting from its receiving. 1 day is by default. After specified period, notification is marked as outdated and deleted according to the **Purge outdated messages** task in the **Server** schedule settings.

  For notifications that received by this sending method, you can specify unlimited storing time in the Web Console Notifications section.
- **Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

Notifications Using Windows Messenger

Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.

Windows Vista OS and later do not support Windows Messenger service.

For notifications in a Windows OS network, specify the following parameters:

- **Resends number** – the number of retries when failed to send a message. Default is 10.
- **Resend time-out** – period in seconds, after which the repeated attempt to send a message is performed. Default is 300 seconds.
- the list of names of computers to receive messages. Only one computer name per each field. To add one more receiver field, click . To remove the field, click .
- **Send test message** – send the test message according to the specified settings of notification system. The test message text is specified in notifications templates.

7.7.2. Web Console Notifications

Via the **Control Center**, you can view and manage administrator notifications which are received via the **Web console** method (sending of administrator notifications is displayed in the Notifications Configuration section).

To view and manage notifications:

1. Select the **Administration** item in the main menu of the **Control Center**. In the opened window, select **Web console notifications** in the control menu. The list of notifications which were sent to the **Web console** will be opened.
2. To vie the notification, click corresponding row of the table. The window with notification texts will be opened. At this, notification will be automatically marked as read.
3. To manege notifications list, use the following elements:

   a) General elements on the toolbar are used to manage notifications section in general. These tools are always available on the toolbar.

Table 7-6. Toolbar elements for managing Web console notifications section

Option		Action
Severity	**Maximal**	Display only notifications with the **Maximal** severity.
	High	Display notifications with severity from **High** to **Maximal**.
	Medium	Display notifications with severity from **Medium** to **Maximal**.
	Low	Display notifications with severity from **Low** to **Maximal**.
	Minimal	Display all notifications with severity from **Minimal** to **Maximal**.
Source	**Agent**	Display notifications related to events on stations
	Server	Display notifications related to events on **Server**

To view notifications that were received during specific time period, use one of the following ways:

- Select from the drop-down list on the toolbar, one of the predefined time periods.
- Select from the drop-down calendars arbitrary dates of beginning and ending of time period.

After editing these settings values, click **Update** to view notifications list according to the specified settings.

b) To manage separate notifications, set the flags next to the necessary notifications or the common flag in the table header to select all notifications from the list. At this, elements on the toolbar to manage selected notifications become available:

Delete notifications - delete all selected notifications without possibility of restore.

Mark notifications as read - mark all selected notifications as read.

c) Set the **Store message without automatic deletion** icon in the notifications list next to those notifications that should not be deleted after expiration of storage period (storage period is set before sending notification in the Notifications Configuration section in the **Web console** sending method settings). Such notifications are stored until you delete them manually in the **Web console notifications** section or clear the icon next to these notifications.

7.7.3. Unsent Notifications

Via the **Control Center** you can track and manage administrative notifications failed to be sent according to the settings of the Notification Configuration section.

To view and manage unsent notifications:

1. Select the **Administration** item in the main menu of the **Control Center**. In the opened window, select **Unsent Notifications** in the control menu. The list of unsent notifications of this **Server** will be opened.
2. To the unsent notifications list whose notifications are placed that was failed to be sent to the recipients, but number of resend attempts which is specified in this notification settings is not yet expired.
3. The table of unsent notifications contains the following information:
   - **Notification** - the name of notification from the list of preinstalled notifications.
   - **Title** - the name of notification block according to whose settings this notification is sent.
   - **Resends remained** - number of remained resend attempts that are taken after notification send failed. Initial number of resend attempts is specified at notifications setup in the Notification Configuration section. After notification has been sent, you cannot change the number of remained resends for this notification.
   - **Time of next resend** - date and time of the next notification resend attempt. Period to perform notification resend attempts is specified at notifications setup in the Notification Configuration section. After notification has been sent, you cannot change the period of remained resends for this notification.
   - **Receiver** - addresses of notification receivers.
   - **Error** - error that caused the failure of notification sending.
4. To manage unsent notifications:
   a) Set the flags next to the specific notifications of the flag in the notifications table header to select all notifications in the list.
   b) Use the following buttons on the toolbar:

      Resend - send selected notifications immediately. At this, the immediate attempt to send the notification is performed. If the sending failed, the number of remained attempts is decremented by one and the time of the next attempt will be counted from the moment of the current sending with periodicity specified in the Notification Configuration section.

      Delete - permanently delete all selected unsent notifications.
5. Unsent notifications are removed from the list in the following cases:
   a) Notification is successfully sent to the receiver.
   b) Notification is deleted by administrator manually via the **Delete** button on the toolbar.
   c) The number of resend attempts is over and notification was not sent.
   d) In the Notification Configuration section, the notification block according to whose settings this notifications have been sending, is removed.

7.8. Administration of Dr.Web Server Repository

The *repository* of **Dr.Web Server** is designed to store benchmark copies of the anti-virus software and update them from **GUS** servers.

The repository deals with sets of files (*products*). Each product resides in a separate subfolder of the repository folder located in the `var` folder, which in case of installation with the default settings is lodged in the **Server** root folder. In the repository each product is dealt with separately.

To administrate the updating in the repository product *revisions* are used. A revision is a correct state of product files at a certain time (including file names and checksums) and has its unique number.

The repository synchronizes revisions of products as follows:

a) to **Dr.Web Server** from the product update site (via HTTP),

b) between different **Dr.Web Servers** in a multi-server configuration according to a specified synchronization policy,

c) from **Dr.Web Server** to workstations.

The repository allows to set up the following parameters:

- the list of product update sites in **a)** operations,
- restrictions to the number of products requiring synchronization of **a)** type (thus, a user is enabled to track only necessary changes of certain files or categories of files),
- restrictions to product components requiring synchronization of **c)** type (a user can choose what should be installed on the workstation),
- control of switching to new revisions (independent testing of products before installation is possible),
- adding one's own components to products,
- independent creation of new products which will be synchronized too.

The **Server** repository deals with the following products:

- **Dr.Web Server**,
- **Dr.Web Agent** (the **Agent** software, the anti-virus software for workstations under corresponding operation systems),
- **Dr.Web Proxy server**,
- **Dr.Web** virus data bases,
- **SpIDer Gate** bases,
- **Dr.Web Anti-spam** bases,
- **Doctor Web** company news.

7.8.1. Repository State

To view the repository state or update anti-virus network components

1. Select the **Administration** item in the main menu of the **Control Center** and click **Repository state** in the control menu of the opened window.
2. In the open window, you can view the list of products in the repository, date of the used revision, date of the last downloaded revision, and products current status.
3. To manage the repository contents, use the following buttons:
   - Click the **Check for updates** button to check whether updates to all of the products are available on the **GUS** servers and download updates, if any.
   - Click **Reload repository from disk**, to reload the current version of the repository from disk.

   On startup, **Server** loads the repository contents to the memory. If during **Server** operation the administrator changed the contents bypassing **Control Center**, e.g, when updating the repository using an external utility or manually, reload the repository to enable the use of its downloaded version.

7.8.2. Delayed Updates

In the **Delayed Updates** section, you can view the list of products which updating is temporarily disabled on the following page: **Detailed repository configuration** → *<Product>* → Delayed Updates. A delayed revision is considered *frozen*.

The table of frozen products contains the following information:

- **Repository folder** - name of the folder where a frozen product resides:
  - 10-drwgatedb - **SpIDer Gate** bases,

- 10-drwspamdb - **Anti-spam** bases,
- 20-drwagent - **Dr.Web Agent** for Windows,
- 20-drwandroid - **Dr.Web Agent** for Android,
- 20-drwcs - **Dr.Web Server**,
- 20-drwunix - **Dr.Web Agent** for UNIX,
- 80-drwnews - **Doctor Web** News.

◆ **Revision** - number of the frozen revision.

◆ **Delayed till** - time until update of the product is delayed.

When clicking the table row, another table with detailed information on the frozen revision of the corresponding product opens.

The option to delay updates is useful when you need to temporarily cancel distribution of last product revision on all stations of the anti-virus network, e.g., if you want to perform preliminary testing of this revision on a limited number of stations.

To use delayed updates functions, perform the actions described in the **Detailed repository configuration** → Delayed Updates section.

To manage delayed updates

1. Set the flags next to the products, for which you want to specify actions on delayed updates. To select all products, set the flag in the heading of frozen products table.
2. On the toolbar, select the required action:

   Execute immediately - disable the frozen state for the product and add the revision to the list of revisions propagating according on stations according to the general procedure.

   Cancel update - disable the frozen state for the product and forbid the revision. Updating from the **GUS** will be restored. The unfrozen revision will be removed from the product revision list. Upon receipt of the next revision, the unfrozen one will be removed from the disk.

   Change updates delay time - specify the time period for the product revision to be delayed. The reference time for a freeze is the moment of receiving the revision from the **GUS**.
3. If you did not specify an action to be applied upon removal of the frozen status, the revision becomes unfrozen when the time is out and is included to the list of revisions distributed to stations according to the general procedure.

7.8.3. General Repository Configuration

In the **General repository configuration** section, you can specify parameters for connection to **GUS** and for updating repositories of all products.

To edit repository configuration

1. Select the **Administration** item in the main menu of the **Control Center**.
2. In the opened window, select the **General repository configuration** item in the control menu.
3. Configure all necessary parameters for updating from the **GUS** as described below.
4. If during parameters editing you need to discard all changes, use the following buttons on the toolbar:

   Reset all parameters to initial values - rerestore the values that all parameters in this section had before current editing. To apply the similar action to a certain parameter value, use the button next to each parameter.

   Reset all parameters to default values - restore all parameters from this section to their defaults, specified in the **Server** configuration file. To apply the similar action to a certain parameter value, use the button next to this parameter.

5. Click one of the following buttons on the toolbar:
   - **Save and resynchronize** - save all changes and update the repository from **GUS** according to the new settings.
   - **Save and reload from disk** - save all changes without updating the repository from **GUS**. At that, the current version of the repository is reloaded from the disk (see also Repository state).

Configuring Dr.Web GUS

On the **Dr.Web GUS** tab, you can configure parameters for connection to **Dr.Web Global Update System**.

To edit GUS connection settings, use the following options:

- In the **Base URI** field, specify the **GUS** servers folder where updates of **Dr.Web** products are located.
- Set the **Use CDN** flag to allow receiving updates from GUS via Content Delivery Network.
- Set the **Use SSL** flag to update repository from GUS via protected SSL connection.

  At this, in the **Allowed certificates** list, select SSL certificates that will be automatically accepted.
- If necessary, edit the list of **GUS** servers from which the repository is updated, in the **Dr.Web Global Update System Servers List** section:
  - To add a **GUS** server to the list of servers used for updates, click and specify the address of the **GUS** server in the appeared field.
  - To remove a **GUS** server from the list of used, click next to the server which you want to delete.
  - **GUS** servers are listed in the order **Dr.Web Server** contacts them when updating the repository. To change the order of **GUS** servers, move a server as necessary by dragging the left root line of the server.

  After installation of **Dr.Web Server**, the list contains only update servers of the **Doctor Web** company. If necessary, you can setup your own update zones and include them into the list of servers to receive updates.

Dr.Web Agent Update Settings

Update of the **Agent** software and anti-virus package is configured separately for different versions of OS under which this software will be installed:

- On the **Dr.Web Agent for Windows** tab, in the group of selection buttons, specify whether you want to update all components that will be installed on stations under Windows OS or update only virus databases.
- On the **Dr.Web Agent for UNIX**, specify UNIX system-based OS for which you want to update the components that are installed on workstations.

To disable all updates receiving from **GUS** for **Agent for UNIX**, open the **Detailed repository configuration** section, the **Dr.Web Agent for UNIX** item, and on the **Synchronization** tab, set the **Disable product update** flag.

Dr.Web Server Update Settings

On the **Dr.Web Server** tab, specify OS for which you want to update **Server** files.

- To receive updates for **Servers** under all supported OS, set the **Update all platforms available on GUS** flag.

- To receive updates for **Server** under certain OS, set only flags located next to their names.

> To disable all updates receiving from **GUS** for the **Server**, open the **Detailed repository configuration** section, the **Dr.Web Server** item, and on the **Synchronization** tab, set the **Disable product update** flag.

News of Doctor Web

On the **Doctor Web News** tab, specify a list of languages for the news feed.

You can configure subscription settings on news lines at the Preferences → **Subscription** section.

You can read news of **Doctor Web** company in the main menu of the **Control Center**, in the **Help** → **News** section.

Languages of Dr.Web Agent for Windows

On the **Dr.Web Agent for Windows languages** tab, specify languages for the **Agent** and the anti-virus package interface of Windows OS, which will be downloaded from the **GUS**.

7.8.4. Detailed Repository Configuration

The **Detailed repository configuration** section provides you with options to configure revision for each repository product separately.

To edit repository configuration

1. Select the **Administration** item on the main menu of the **Control Center**.
2. In the opened window, select in the **Detailed repository configuration** subsection of the control menu, the item, which corresponds to the product you want to edit.
3. Configure all necessary repository settings for the selected product, described below.
4. Click **Save and reload from disk** on the toolbar to save all your changes. At that, the current version of the repository is reloaded from the disk (see also Repository state).

Revision List

On the **Revision list** tab, you can view information on all revisions available on the **Server** for this product.

The table of revisions contains the following columns:

Column name	Description
Distributed	Automatic marker in this column defines the state of product revisions. Two types of markers are available: - *Distributed revision*. Revision used for updating **Agents** and anti-virus software on the workstations. Revision for distribution is selected as follows: 1. Revision indicated with the marker in the **Current** column is distributed. Only one revision can be marked. For the **Dr.Web Agent for Windows** product, revision received earlier than the current one cannot be selected as distributed.

Column name	Description
	2. If no revision is marked in the **Current** column, the revision indicated with the marker in the **Stored** column is distributed. 3. If no revision is marked in the **Current** and **Stored** columns, the last revision is distributed. The automatic marker always indicates the distributed revision. - *Frozen revision*. A frozen revision is not distributed to stations, new revisions are not downloaded from the **Server**. For actions under frozen revision, refer to Delayed Updates. If a revision is frozen, the revision for distribution is selected as follows: 1. If the marker in the **Current** column is set, the current revision is distributed to stations. 2. If the marker in the **Current** column is not set, the revision that precedes the current one is distributed to stations.
Current	Set the marker to specify the revision used for updating **Agents** and anti-virus software on the stations. Only one revision can be selected as current. Alternatively, a marker that indicates the current revision can be not set.
Stored	Set the marker to save the revision when the repository is automatically cleaned up. The marker can be set for different revisions simultaneously. Alternatively, a marker can be not set. **Server** stores a certain number of product revisions which is specified on the **Synchronization** tab. When the specified number of maximal stored revisions is reached, the oldest temporarily stored revision is deleted upon saving a new one, downloaded from the **GUS**. When the repository is automatically cleaned up, the following revisions are not removed: • Revisions indicated with marker in the **Stored** column. • Revision indicated with marker in the **Current** column. If the product revision is stable, you can mark it as stored and in case a new revision, downloaded from **GUS**, is unstable, you will be able to rolle back to the previous one.
Revision	The date the product revision was received. If the revision is frozen, the blocking status displays in the column as well.

Synchronization

On the **Synchronization** tab, you can configure parameters for updating the **Server** repository from **GUS**:

- In the **Stored revisions number** drop-down list, number of product revisions temporary stored on disk not including revisions which are marked at least in one column of the **Revisions list** tab. When a new revision is received and the number of stored revisions already reached the specified value, the oldest revision is removed. Revisions marked as **Current**, **Stored** and **Distributed** are not removed.
- Set the **Disable product update** flag to disable receiving updates for this product from the **GUS** servers. **Agents** will be updated to the current revision on the **Server** (or according to the procedure used to select the distributed revision).

For some products, the following settings are also available:

- Set the **Update only following files** flag to receive updates from **GUS** only for the file listed below.
- Set the **Do not update only following files** flag to disable updating from **GUS** only for the file listed below.

Files can be specified in the format of regular expressions.

If both flags are set, files for an update are selected as follows:

1. From the full list of product files only those are selected that are specified in the **Update only following files** lists.
2. From the selection at step 1, files specified in the **Do not update only following files** lists are removed.
3. Files resulting from the selection at step 2 are updated from **GUS**.

Notifications

On the **Notifications** tab, you can configure notifications on repository updates:

- Set the **Do not notify only about following files** flag to disable notifications on events of the files listed below.
- Set the **Notify only about following files** flag to enable notifications on events of the files listed below.

  Files can be specified in the format of regular expressions.

If exceptions list are not specified, all notifications enabled on the Notifications configuration page are sent.

Parameters of notifications on repository updates are configured in the Notifications configuration page, in the **Repository** section.

Delayed Updates

On the **Delayed updates** tab, you can delay distribution of updates on stations for the specified period of time. A delayed revision is considered *frozen*.

The option to delay updates is useful when you need to temporarily cancel distribution of last product revision on all stations of the anti-virus network, e.g., if you want to perform preliminary testing of this revision on a limited number of stations.

To use delayed updates functional, perform the following actions:

1. For the product, update of which you want to freeze, configure delayed updates as described below.
2. To disable distribution of the last revision, set one of the previous revisions as a current on the Revision list tab.
3. For the group of stations that will receive the last revision, set the **Receive all the latest updates** flag on the **Anti-virus Network** → Update Restrictions for Workstations section. Other workstations will receive the revision which you selected as current at step 2.
4. The next downloaded from the **GUS** revision which is satisfying the conditions specified for the **Delay updates for the following files only** option, will be frozen and delayed for the time period specified in the **Change updates delay time** list.

To configure delayed updates:

1. Set the **Delay updates** flag to temporarily disable downloading updates from **GUS** servers for this product.
2. In the **Updates delay time** drop-down list, select the time period to delay downloading of updates starting from the moment of their receive from the **GUS** servers.
3. If required, set the **Delay updates for the following files only** flag to delay distribution of updates that contain files which corresponds to the masks specified below. Masks are specified in the format of regular expressions.

If the flag is cleared, all updates from the **GUS** are frozen.

To disable the frozen state:

- On the **Revision list** tab, click **Execute immediately** to disable the frozen state for the product and add the revision to the list of revisions distributed to stations according to the general procedure.
- On the **Revision list** tab, click **Cancel update** to disable the frozen state for the product and forbid the revision. Updating from the **GUS** is restored. Unfrozen revision will be removed from the list of product revisions. After the next revision is received, the unfrozen revision will be removed from the disk.
- When the time specified in the **Change updates delay time** list is out, the revision becomes unfrozen and is included to the list of revisions distributed to stations according to the general procedure.

You can manage frozen revisions for all products on the Delayed Updates page.

7.8.5. Repository Content

The **Repository content** section allows to view and manage current repository content as files and folders of repository folder.

The main window of **Repository content** section contains hierarchical tree of repository content displays all folders and files of current version of the repository with the list of all revisions for each product.

View Information on the Repository

To view information on all repository objects, select the object in the hierarchical tree of repository content. The properties panel with the following information will be opened:

- The **Selected objects** subsection contains detailed information on the object selected in the repository content tree: **Type**, **Size** (for separate file only), **Creation date** and **Modification date**.
- The **Repository state** subsection contains general information on all repository objects: current list of objects and the date of their last update.

Manage Repository

To manage repository content, use the following buttons on the toolbar:

Export repository file to an archive,

Import archive with repository files,

Delete selected objects - delete objects selected in the repository content tree without possibility to restore.

After you change the repository content, e.g. delete or import repository objects, to use the changed data by the **Server** you must reload the repository.

See the Repository State section.

Repository Export

To save repository file into a zip archive, perform the following actions:

1. In the hierarchical tree of the repository content, select the product, separate product revision or entire repository. Entire repository will be exported if nothing is selected in the tree or the **Repository** tree header is selected. To select several objects, use CTRL or SHIFT.

   Please note the general type of exported objects during repository export:

   a) Zip archives of repository products. Such archives contains one of the following repository object types:
   - Entire repository.
   - Entire product.
   - Entire separate revision.

   Archives generated during export of these objects can be imported via the **Repository content** section. The name of such archives contains the `repository_` prefix.

   b) Zip archives of separate repository files.

   Archives generated during export of separated files and folders which are lower than objects from the **a)** item in the hierarchical tree, cannot be imported via the **Repository content** section. The name of such archives contains the `files_` prefix.

   Such archives can be used as backup copies of files for manual replacement. But it is not recommended to replace repository files manually, bypassing the **Repository content** section.

2. Click **Export repository file to an archive** on the toolbar.
3. Specify the path to save zip archive with selected repository object according to the web browser settings in which the **Control Center** is opened.

Repository Import

To load repository files from a zip archive, perform the following actions:

1. Click **Import archive with repository files** on the toolbar.
2. In the opened window, in the **Select file** section, specify the zip archive with repository files. To select the file you can use the button.

   You can import only those zip archives that have been collected during the export of one of the following repository object types:

   - Entire repository.
   - Entire product.
   - Entire separate revision.

   The name of such archives during export contains the `repository_` prefix.
3. In the **Import settings** section, specify the following parameters:
   - **Add missing revisions only** - in this import mode, only those revisions of repository will be added that are missing in the current version. Other revisions remain unchanged.
   - **Replace entire repository** - in this import mode, repository is fully replaced with the imported one.
   - Set the **Import configuration files** flag to import configuration files when importing repository.
4. Click **Import** to start the import process.

7.9. Additional Features

7.9.1. Database Management

The **Database management** section allows to perform direct maintenance of the database with which **Dr.Web Server** is operated.

The **General** section contains the following parameters:

- The **Last DB maintenance** field - the date of last execution of the database maintenance commands from this section.
- The list of commands to maintain the database which includes:
  - Commands similar to the tasks from Dr.Web Server schedule. The names of commands correspond to the names of tasks in the **Action** section of the **Server** schedule (description of corresponding schedule tasks is given in the Tasks types and their parameters table).
  - The **Analyse database** command. It is designed to optimize the **Server** database using the `analyze` command.

To execute database maintenance commands

1. In the commands list, set the flags for the commands you want to execute.

   If necessary, change the time periods for the database purging commands, after which stored information is confirmed outdated and should be removed from the **Server**.

2. Click **Apply now**. All selected commands will be executed immediately.

   For postponed or/and periodic automatic execution of these commands (except **Analyse database**), use Server Task Scheduler.

To manage database use the following buttons on the toolbar:

Import,

Export,

Backup.

Database Export

To save the database information into a file, perform the following actions:

1. Click **Export** on the toolbar.
2. In the export settings configuration window, select one of the following variants:
   - **Export entire database** to save all information from the database into a gz archive. Exported XML file is similar to the database export file which is obtained when running the **Server** executable file from the command line with the `xmlexportdb` switch. This export file can be imported when running the **Server** executable file from the command line with the `xmlimportdb` switch.
     These commands are described in details in the **Appendices** documents, in the H3.3. Database Commands section).

- **Export information on stations and groups** to save information about the objects of the anti-virus network into a zip archive. In the result of this command execution, all information on groups of stations and stations accounts of the anti-virus network served by this Servers, is save into the file of a specific format. Export file contains the following information about stations: properties, components configuration, permissions, update restrictions settings, schedule, installing components list, statistics, information on deleted stations; about groups: properties, components configuration, permissions, update restrictions settings, schedule, installing components list, parent group ID.
  Further, export file can be imported via the **Database management** section.

3. Click **Export**.
4. Specify the path to save the archive with the database according to the web browser settings in which the **Control Center** is opened.

Database Import

You can use the import procedure of the database containing information on the objects of anti-virus network, to transfer the information either on the new **Server** or on the **Server** which is already operating into anti-virus network, particularly to merge the lists of served stations of two **Servers**.

All imported stations will be able to connect to the **Server** on which you perform the import. When you performing the import, please note that you must have corresponding number of available licenses to connect imported stations. E.g., if necessary, in the License Manager section, add the license key from the **Server**, from which the information about stations had been imported.

To load the database from a file, perform the following actions:

1. Click **Import** on the toolbar.
2. In the import window, specify the zip archive with the database file. To select the file, you can use the button.

   You can import only those zip archives that have been obtained during the export of the database for the **Export information on stations and groups** option.

3. Click **Import** to start the import process.
4. If during import, there are stations or/and groups with the same identifiers which are included both into imported data and into current **Server** database, the **Collisions** section opens to configure actions on duplicated objects.

   Groups and stations lists are presented in separated tables.

   For corresponding objects table, in the **Groups import mode** or **Stations import mode** drop-down list, select one of the collision resolving option:

   - **Save import data for all** - delete all information on duplicated objects from the current **Server** database and overwrite it with the information from the imported database. The action is applied simultaneously to all duplicated objects in this table.
   - **Save current data for all** - save all information on duplicated objects from the current **Server** database. Information on duplicated objects from the imported database will be ignored. The action is applied simultaneously to all duplicated objects in this table.
   - **Select manually** - specify the action for each duplicated objects manually. In this mode, the list of duplicated objects become editable. Set the options for those objects, which will be saved.

   Click **Save**.

Back up

To back up **Server** critical data, click **Backup** on the toolbar. The data will be saved into gz archive. Backup files are similar to files which are obtained when running the **Server** executable file from the command line with the `backup` switch.

This command is described in details in the **Appendices** documents, in the H3.5. Backup of Dr.Web Server Critical Data.

7.9.2. Dr.Web Server Statistics

Via the **Control Center**, you can view the statistics on **Dr.Web Server** operating on the level of system resources usage of a computer on which **Dr.Web Server** is installed and also network interaction with anti-virus network components and external resources such as **GUS**.

To view Dr.Web Server operation statistics:

1. Select the **Administrating** item in the main menu of the **Control Center**.
2. In the opened window, select the **Dr.Web Server statistics** item of the control menu.
3. In the opened window, the following statistic data sections are presented:
   - **Customer activity** - data on number of served clients, which are connected to this **Server**: **Dr.Web Agents**, neighbor **Dr.Web Servers** and **Dr.Web Agent** installers.
   - **Network traffic** - parameters of incoming and outgoing network traffic for exchanging data with the **Server**.
   - **System resources usage** - usage parameters of system resources of the computer on which the **Server** is installed.
   - **Microsoft NAP** - Dr.Web NAP Validator operation parameters.
   - **Database usage** - parameters of the **Server** database accessing.
   - **File cache usage** - parameters of accessing the file cache of the computer on which the **Server** is installed.
   - **DNS cache usage** - parameters of accessing the cache which stores queries to DNS servers on the computer on which the **Server** is installed.
   - **Alerts** - parameters of the administrative notifications subsystem operation.
   - **Repository** - parameters of data exchange between the **Server** repository and **GUS** servers.
   - **Web statistics** - parameters of usage of the **Web server**.
   - **Cluster** - parameters of accessing via the interserver synchronization protocol in **Servers** cluster system for multiserver network configuration.
4. To view statistic data of specific section, click the section name.
5. In the opened list, the section parameters with dynamic counters of values are given.
6. At the statistic section opening, the graphical representation for each parameter changes is enabled. At this:
   - To disable graphical representation, click the section name. When graphical representation is disabled, the digital value of parameters still dynamically refreshes.
   - To enable graphical representation of the data repeatedly, click the section name ones more.
   - The names of the sections and their parameters for which the graphical representation is enabled, are marked with the bold font.
7. To edit the parameters refresh frequency, use the following toolbar options:
   - In the **Refresh rate** drop-down list, select the necessary data refresh frequency. After the drop-down list value changed, the time period of digital and graphical data refreshing is automatically applied.
   - Click **Refresh** to refresh all statistic data values at a time.

8. On mouse hover over the graphical data, the selected point digital value is displayed as the following:
   - **Abs** - parameter absolute value.
   - **Delta** - incrementation of the parameter value relative to its previous value according to the data refresh rate.
9. To hide the section parameters, click the arrow on the left of the section name. When the section parameters are hidden, the graphical statistic data is cleared and on the parameters opening, the drawing starts from the beginning.

7.9.3. Backups

The **Backups** section allows to view as files and folders and also save locally contents of **Dr.Web Server** critical data backup copies.

During backup, the following objects are saved: repository settings, configuration files, encryption keys, certificates, embedded database backup.

Dr.Web Server critical data backup copies are saved in the following cases:

- As a result of the **Back up critical server data** task execution according to the **Server** schedule.
- As a result of back up when running the **Server** executable file from the command line with the `backup` switch. This command is described in details in the **Appendices** documents, in the H3.5. Backup of Dr.Web Server Critical Data.

View Information on Backups

To view information on the backup, select the object in the hierarchical tree of the backups. The properties panel with the following information on the object will be opened: **Type**, **Size** (for separate file only), **Creation date** and **Modification date**.

Manage Backups

To manage backups, use the following buttons on the toolbar:

Export - allows to save the backup of selected object to the computer on which the **Control Center** is opened.

Delete selected objects - delete objects selected in the tree without possibility to restore.

Backup Export

To save the backup locally, perform the following actions:

1. In the hierarchical tree, select the necessary backups (to select entire backup, it is enough to select in the tree the folder that corresponds to this backup), or separate files from the backup composition. To select several objects, use CTRL or SHIFT.

   Please note the general type of exported objects during the export:

   a) Zip archives of the backups are saved for the following selected objects:
      - One or several entire backups (when selecting folders which correspond to the backups).
      - Several separate files from the backups composition.

   b) Separate files from the backups composition. If only one file have been selected for the export, it will be saved as it is without archiving.
2. Click **Export** on the toolbar.

3. Specify the path to save selected objects according to the web browser settings in which the **Control Center** is opened.

7.10. Peculiarities of a Network with Several Dr.Web Servers

Dr.Web Enterprise Security Suite allows to build an anti-virus network with several **Dr.Web Servers**. In such networks each workstation is assigned to one **Server**, which allows to distribute the load between them.

The connections between the **Servers** can have an hierarchical structure, which allows optimally distribute the load between the **Servers**.

To exchange information between the **Servers** a special *interserver synchronization protocol* is used.

Features provided by interserver synchronization protocol:

- Distributing updates between **Servers** within anti-virus network.
- Immediate transmission of updates as soon as they are received from **Dr.Web GUS** servers.
- Transmitting statistic information on protection stations states between connected **Servers**.
- Transmitting licenses for protected stations between neighbor **Servers**.

7.10.1. Building a Network with Several Dr.Web Servers

Several **Dr.Web Servers** can be installed in an anti-virus network. Each **Dr.Web Agent** connects to one of them; each **Server** with connected anti-virus workstations functions as a separate anti-virus network as described in previous Chapters.

Dr.Web Enterprise Security Suite allows to connect such anti-virus networks by transferring data between **Dr.Web Servers**.

Dr.Web Server can send to another Dr.Web Server

- software and virus database updates (only one of them is to receive updates from **Dr.Web GUS** servers);
- information on virus events, statistics, etc.;
- licenses for protected stations (you can configure licenses propagation between **Servers** in the License Manager).

The program provides for two types of connections between Dr.Web Servers:

- a *parent-child* type of connection, where the principle **Server** transfers updates to the subordinate one and receives information about events,
- a *peer to peer* connection, where data types and transfer directions are set up individually.

An example of a multi-server structure is presented in Figure 7-1.

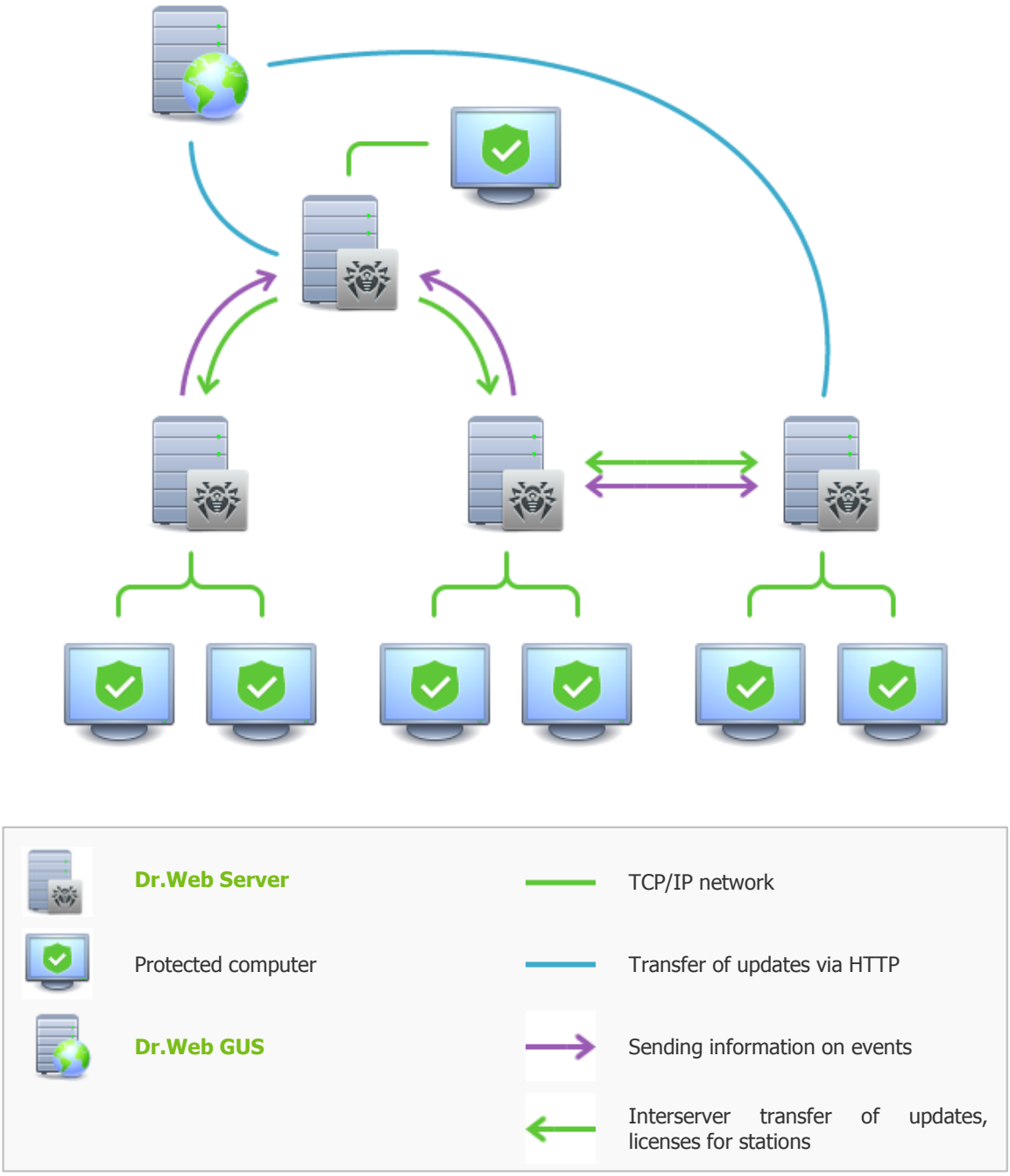


Figure 7-1. A multi-server network

Some advantages of the anti-virus network with several Dr.Web Servers:

1. Receiving of updates from **Dr.Web GUS** servers by one principle **Dr.Web Server** and their subsequent distribution to the other **Servers** directly or through intermediates.

Servers that receive updates from the superior **Server**, do not receive updates from **GUS** even if such task is set in the schedule.

Still, in case the parent **Server** is inaccessible, it is recommended to keep the task for updating from the **GUS** on subordinate **Servers**. This allows the **Agents** which are connected to the subordinate **Server** to receive updated virus databases and program modules (see also p. General Repository Configuration).

In the task for updating from **GUS** on the superior **Server** propagating updates, you must set up the receiving updates of the **Server** software for all operating systems installed on all subordinate **Servers**, which receive updates from this superior **Server** (see p. General Repository Configuration).

2. Distribution of workstations between several **Servers**, decreasing the load on each of them.
3. Consolidation of data from several **Servers** on one **Server**; the possibility to view all the data through **Dr.Web Security Control Center** connected to such **Server**.

Dr.Web Enterprise Security Suite anti-virus monitors and prevents the creation of cyclic data flows.

4. Available licenses for protected stations can be donated to the neighbor **Server**. At this, the license key itself remains at the disposal of the distributing **Server**, available licenses are propagated to a neighbor **Server** for a specified time period and after it has expired, the licenses are revoked.

7.10.2. Setting Connections between Several Dr.Web Servers

To use several **Servers** in an anti-virus network, you should set up connections between these **Servers**.

It is advisable to make a plan of the anti-virus network structure first. All data flows, connections of the "peer to peer" and "parent-child" types should be indicated. Then, each **Server** included into the network connections with any "neighboring" **Servers** ("neighbors" have at least one dataflow between them) should be set up. After that, for each **Server** included into the network, you should set up connections with "neighboring" **Servers** ("neighbors" have at least one data flow between them).

Example of configuring of a connection between Parent and Child Dr.Web Servers

Values of fields, marked by the * sign, must be obligatory specified.

1. Make sure that both **Dr.Web Servers** operate normally.
2. To each of **Dr.Web Servers** give "meaningful" names, as it will help prevent mistakes while connecting and administering **Dr.Web Servers**. You can change the names through **Dr.Web Security Control Center** menu: **Administration** → **Dr.Web Server configuration** on the **General** tab in the **Name** field. In this example we name the parent **Server** `MAIN`, and the child **Server** - `AUXILIARY`.
3. On both **Dr.Web Servers**, enable the **server** protocol. To do this, on **Dr.Web Security Control Center** **Administration** menu, select **Dr.Web Server configuration**. On the **Modules** tab, set the **Dr.Web Server protocol** flag (see p. Modules).

If the server protocol is disabled, the message about enabling this protocol will be shown and the link to the corresponding section of **Dr.Web Security Control Center** will be given during creation of new connection.

4. Restart both **Dr.Web Servers**.
5. Via **Dr.Web Security Control Center** of the child **Server** `(AUXILIARY)`, add the parent **Server** `(MAIN)` to the list of neighbor **Servers**. To do this, select **Neighborhood** item in the main menu. A window with the hierarchical list of the anti-virus network **Servers** "neighboring" with the given **Server** will be opened. To add a **Server** to the list, click the **Create neighbor** on the toolbar.

   A window to describe the connection between the current and the new **Server** will be opened. Specify the following parameters:

- **Type** of creating neighbor is **Parent**.
- **Name** - the name of the parent **Server** (`MAIN`).
- **Password*** - an arbitrary password to access the parent **Server**.
- **Own keys of Dr.Web Server** - the list of public encryption keys of configuring **Server**. Click and specify the `drwcsd.pub` key of the current **Server**. To add one more key, click and add the key to the new field.
- **Keys of neighbor Dr.Web Server*** - the list of public encryption keys of connecting parent **Server**. Click and specify the `drwcsd.pub` key of the parent **Server**. To add one more key, click and add the key to the new field.
- **Address*** - the network address of the parent **Server** and the connection port. Use the following format: <*Server_address*>:<*port*>.

You can browse the list of **Servers**, available in the network. To do this:

a) Click the arrow on the right of the **Address** field.

b) In the opened window, specify networks in the following format: with a hyphen (for example, `10.4.0.1-10.4.0.10`), separated by a comma with a whitespace (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), with a network prefix (for example, `10.4.0.0/24`).

c) Click to browse the network for available **Servers**.

d) Select the **Server** in the list of available **Servers**. Its address will be set to the **Address** field to create connection.

- **URL of Dr.Web Security Control Center** - you can specify the address of a start web page for **Dr.Web Security Control Center** of the main **Server** (see p. Dr.Web Security Control Center).
- In the **Connection parameters** drop-down lists, specify the type of creating neighbor **Servers** connection.
- In the **Encryption** and **Compression** drop-down lists, specify parameters of traffic encryption and compression between connecting **Servers** (see p. Traffic Encryption and Compression).
- **Validity period of donated licenses** - time period on which licenses are donated from the key on the parent **Server**. The setting is used if the parent **Server** donates licenses to the current **Server**.
- **Period for accepted licenses renewal** - the setting is not used in creating a parent **Server**.
- **License synchronization period** - interval for synchronizing information about donating licenses between **Servers**.
- Flags in **Licenses**, **Updates** and **Events** sections are set according to *parent-child* type of connection and can not be changed:
  - parent **Server** sends licenses to child **Servers**;
  - parent **Server** sends updates to child **Servers**;
  - parent **Server** receives information about events from child **Servers**.
- In the **Update restrictions** > **Events** section, you can configure the schedule of events transmission from the current **Server** to the parent one (events transmission mode can be edited as updates mode in the Update Restrictions for Workstations section).

Click **Save**.

As a result, the Parent **Server** (`MAIN`) will be included to the **Parents** and **Offline** folders (see Figure 7-2).

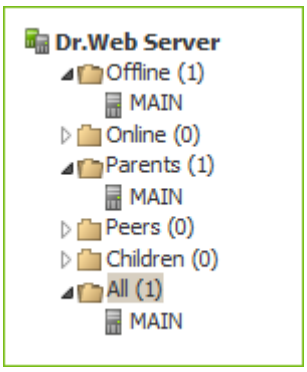


Figure 7-2.

6. Open **Dr.Web Security Control Center** of the parent **Server** (MAIN) and add the child **Server** (AUXILIARY) to the list of neighbor **Servers**. To do this, select **Neighborhood** item in the main menu. A window with the hierarchical list of the anti-virus network **Servers** "neighboring" with the given **Server** will be opened. To add a **Server** to the list, click **Create neighbor** on the toolbar.

   A window to describe the connection between the current and the new **Server** will be opened. Specify the following parameters:

   - **Type** of creating neighbor is **Child**.
   - **Name** - the name of the Child **Server** (AUXILIARY).
   - **Password*** - type the same password as at step **5**.
   - **Own keys of Dr.Web Server** - the list of public encryption keys of configuring **Server**. Click and specify the drwcsd.pub key of the current **Server**. To add one more key, click and add the key to the new field.
   - **Keys of neighbor Dr.Web Server*** - the list of public encryption keys of connecting child **Server**. Click and specify the drwcsd.pub key of the child **Server**. To add one more key, click and add the key to the new field.
   - **URL of Dr.Web Security Control Center** - you can specify the address of a start web page for **Dr.Web Security Control Center** of the child **Server** (see p. Dr.Web Security Control Center).
   - In the **Connection parameters** drop-down lists, specify the type of creating neighbor **Servers** connection.
   - In the **Encryption** and **Compression** drop-down lists, specify parameters of traffic encryption and compression between connecting **Servers** (see p. Traffic Encryption and Compression).
   - **Validity period of donated licenses** - the setting is not used in creating a child **Server**.
   - **Period for accepted licenses renewal** - period till the license expiration, starting from which the child **Server** initiates renewal of the license which is accepted from the current **Server**. The setting is used if the child **Server** accepts licenses from the current **Server**.
   - **License synchronization period** - interval for synchronizing information about donating licenses between **Servers**.
   - Flags in **Updates** and **Events** sections are set according to *parent-child* type of connection and can not be changed:
     - child **Server** receives updates from main **Server**;
     - child **Server** send information about events to main **Server**.
   - In the **Update restrictions** > **Updates** section, you can configure the schedule of updates transmission from the current **Server** to the child one (updates transmission mode can be edited as updates mode in the Update Restrictions for Workstations section).

   Click **Save**.

As a result, the child **Server** (AUXILIARY) will be included to the **Children** and **Offline** folders (see Figure 7-3).

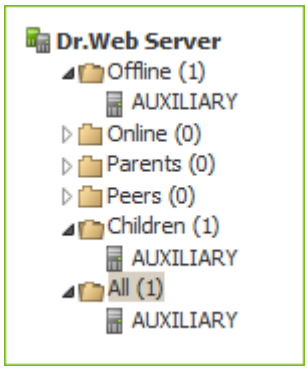


Figure 7-3.

7. Wait until the connection between **Servers** is established (usually it takes not more than a minute). Press F5 from time to time to update the **Servers** list. After the **Servers** have been connected, the child **Server** (AUXILIARY) will move from the **Offline** folder to the **Online** folder (see Figure 7-4).

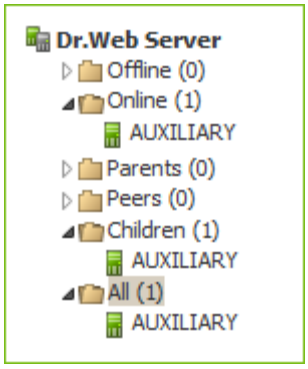


Figure 7-4.

8. Open **Dr.Web Security Control Center** of the child **Server** (AUXILIARY) to make sure that the parent **Server** (MAIN) is connected to the child **Server** (AUXILIARY) (see Figure 7-5).

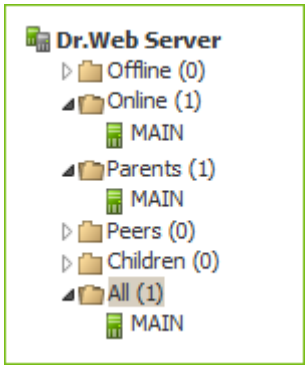


Figure 7-5.

You may not connect several **Servers** with the same pare of parameters: password and the drwcsd.pub public key.

For peer to peer connections between **Servers**, it is recommended to set **Server** address in the settings for one of them only.

It will not take effect on the **Servers** interconnection, but allows to avoid messages like `Link with the same key id is already activated` in the **Servers** log files.

Connection between two Dr.Web Servers can be failed because of:

- Network problems.
- Wrong address of the parent **Server** was set during connection setup.
- Wrong `drwcsd.pub` encryption public keys at one of connecting **Servers**.
- Wrong access password at one of connecting **Servers** (passwords on connecting **Servers** do not match).

7.10.3. Using an Anti-Virus Network with Several Dr.Web Servers

The peculiarity of a multi-server network is that updates from **Dr.Web GUS** servers can be received by a part of **Dr.Web Servers** (as a rule, one or several parent **Servers**) and update tasks should be scheduled on these **Servers** only (for information on how to set **Servers** schedule, read p. Setting Dr.Web Server Schedule). Any **Server** which has received updates from **Dr.Web GUS** servers or some other **Servers** distributes them immediately to all connected child **Servers** and those peer **Servers** for which this option is enabled.

Dr.Web Enterprise Security Suite anti-virus automatically monitors the situations when due to an imperfect structure of the network or incorrect **Server** configuration an update already received is sent again to the same **Server**, and cancels the updating.

The administrator can receive consolidated data about important events on the anti-virus stations linked to any **Server** via intersever connections.

To view information on virus events on all Dr.Web Servers linked to the current Dr.Web Server:

1. Select **Neighborhood** item in the main menu of **Dr.Web Security Control Center**.
2. In the opened window in the **Tables** item of the control menu, select the **Summary data** option to view the data on the total number of entries on events at neighbour **Servers**. In the table with statistic data on neighbour **Servers**, the following data is displayed:
   - **Infections** - infections which are detected at stations, connected to the neighbour **Servers**.
   - **Errors** - scanning errors.
   - **Statistics** - statistics on detected infections.
   - **Start/Stop** - the launch and termination of scan tasks.
   - **Status** - status of anti-virus software on stations.
   - **All network installations** - network installations of the **Agent**.
3. To view the page with detailed tabular information on events at neighbour **Servers**, click the number of entries on demand event at the table in **Summary data** section.
4. Also, to view the page with detailed tabular information on events at neighbour **Servers**, select the corresponding item (see step 2) in the **Tables** section of the control menu.
5. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.
6. To save the table for printing or further processing, click

   Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

7.10.4. Dr.Web Servers Cluster

You must upgrade **Servers** within the cluster from installation packages only. At this, you must stop all the **Servers** and upgrade them one after another. Upgrading via the **Control Center** (transition to a new revision) should not be used because after you upgrade the first **Server** in using the common database, all other **Servers** will not be able to operate and upgrade.

For creation of the **Servers** cluster in the anti-virus network, the following prescriptions must be implemented:

1. The same configuration files

All **Servers** must have the same `drwcsd.pub` and `drwcsd.pri` encryption keys.

If encryption keys have not been created before, during installation of the first **Server** of a cluster, encryption keys will be generated automatically.

You can get necessary encryption keys for installation of the next **Servers** of a cluster, via the **Control Center**: **Administration** > **Encryption keys** menu. At this, depending on the following cluster establishing way, either both keys or only `drwcsd.pri` may be needed:

- If the `drwcsd.pri` private encryption key is specified during the **Server** installation, the `drwcsd.pub` public key is generated automatically.
- If the necessary private key is not specified during the **Server** installation, when you must replace both of the keys manually after the installation.

Location of configuration files is given in the Dr.Web Server section.

2. Common Server name

For all **Servers**, the same IP address or DNS name of the **Server** must be specified to use it for generating **Agent** installation files for an anti-virus network stations.

This name is specified via the **Control Center**: **Administration** > **Dr.Web Server configuration** > the Download tab > the **Dr.Web Server address** field. Settings of this section are stored in the `download.conf` configuration file (description of the file is given in the **Appendices** document, p. G3. Download.conf Configuration File).

3. Cluster usage setup

At the network DNS server, the common cluster name must be registered for each **Server** and load balancing must be set.

For automatically applying of the settings in **Dr.Web Servers** cluster, the specific cluster protocol must be used.

To configure cluster protocol, it is necessary for each **Server** in the **Control Center** open the **Administration** > **Dr.Web Server configuration** menu ans specify the following settings:

a) To enable cluster protocol, on the Modules tab, set the **Dr.Web Servers cluster protocol** flag.

b) To configure parameters for interaction of the **Servers** within a cluster, on the Cluster tab specify the corresponding parameters.

c) After configuring of the necessary parameters, click **Save** and restart the **Servers**.

For Example

- Multicast group: `232.0.0.1`
- Port: `11111`
- Interface: `0.0.0.0`

In this example, for all **Servers** of a cluster, transports for all interfaces are configured. In other cases, e.g., if one of the networks is external for the cluster and the **Agents** are connected from it, and the second network is intercluster, when cluster protocol is better to open only for interfaces of the internal network. In this case, the following addresses must be set as an interfaces: `192.168.1.1`, ..., `192.168.1.N`.

4. *The same database*

To be able to work with a common database, all **Dr.Web Servers** must be the same version.

All **Dr.Web Servers** within one cluster, must operate with the same external database.

As in the case of the database without cluster, each of the **Servers** calls the database independently and all **Servers** data is stored separately. Wherever relevant, **Server** gets from the database only records for its ID which is unique for each **Server**. Usage of the same database allows the **Servers** operate with the **Agents**, firstly registered on other **Servers** of a cluster.

When you creating a **Servers** cluster with the same database, please consider the following features:

- The database may be installed either separately from all **Servers** or on the one of the computers on which the **Server** of a cluster in installed.
- The database must be created before installation of the first **Server** of a cluster or before the connection of the first **Server** to the database.
- When adding new hosts into the cluster (except the first **Server**), during the **Servers** installation it is not recommended to set the common database which is used in this cluster directly. Otherwise, it may cause the deletion of the information already stored into the database. It is recommended to install the **Servers** firstly with an embedded database and after the installation to switch them to the common external database.
  Switch the **Servers** to the external database usage you can via the **Control Center**: in the **Administration** > **Dr.Web Server configuration** > on the Database tab or via the `drwcsd.conf` **Servers** configuration file.
- Except the first **Server** of a cluster, it is not recommended to add the **Servers** already operating within anti-virus network with other external or embedded database to a cluster. It will cause the loss of data: information on stations, statistics, settings (except the settings which are stored in the configuration files), because data are completely erased from the base during the import. In this case, only a part of some of the settings can be imported.

5. *The same version of the repository*

On all **Servers** of a cluster, repositories must contain updates of the same version.

You can reach this requirement by one of the following ways:

- Update all **Servers** of a cluster from the **GUS** simultaneously. In this case, all **Servers** contain the latest version of updates. Update all **Servers** repositories is also can be configured from the local update zone which will distribute the same confirmed version of products updates or the latest version in case if the **GUS** mirror is created.

- It is allowed to create hybrid structure that combines both cluster of the **Servers** and hierarchical structure based on interserver connections. At this, on of the **Servers** (may be either the **Server** within a cluster or not included into a cluster) is assigned as a parent and receives updates from the **GUS**. Other **Servers** of a cluster are the child hosts and receive updates from the parent **Server** via the interserver connections.

If **Servers** of a cluster are configured to receive updates from the local zone (**GUS** mirror) or from the parent **Server**, it is necessary to track functionality of this zone of the parent **Server**. If a host that distributes updates is denied of service, it is necessary to reconfigure one of the other **Servers** to operate as a parent **Server** or create a new update zone to receive updates from the **GUS** correspondingly.

6. Features of licenses distribution for the stations

To distribute licenses between **Servers** of a cluster, you can use the following approaches:

a) Create hybrid structure that combines both cluster of the **Servers** and hierarchical structure based on interserver connections. Such structure is useful if for serving the **Agents** within **Servers** cluster system, the dynamic allocation of stations between **Servers** of a cluster is performed. In this case, the necessary number of licenses are propagated from a parent **Server** (may be either the **Server** within a cluster or not included into a cluster) to child **Servers** via the interserver connection directly during operation.

   Thus, on a parent **Server** can be located only one license file containing the number of licenses that corresponds the total number of server stations, and the necessary number of licenses to child **Servers** is propagated during operation of a cluster. Administrator of anti-virus network should manually configure donation of necessary number of licenses to child **Servers** for a necessary time period.

   Use the License Manager to configure licenses donation to the neighbor **Servers**.

   For example, you can configure hierarchical structure of **Servers** and allocate the parent **Server** (may be either the **Server** within a cluster or not included into a cluster) which will be propagate both repository updates and licenses from a license file to all nodes of a cluster.

b) In case of refusal to configure hierarchical structure of the **Servers**, opportunity to donate licenses from a single license file between all the **Servers** is not supported. In this case, you must plan the structure of anti-virus network considering cluster of the **Servers** beforehand, and use several license files - one for each **Serves** of a cluster. Total number of licenses in all license files is equal to the total number of stations in the network, but distribution the number of licenses between **Servers** of a cluster you must calculate beforehand considering the assumed number of stations that are planned to be connected to each **Server**.

7. Tasks in the Server schedule

To avoid duplicates in queries to the database, it is recommended to execute the following tasks from the **Server** schedule only on the one of the **Servers**: **Purge Old Data**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge unsent IS events**. For example, on the **Server** which is located on the same computer as the common external database. Or on the most productive computer of a cluster, if configuration of the **Servers** are differ and the database is located on the separate computer.

Chapter 8: Updating Dr.Web Enterprise Security Suite Software and Its Components

Before updating **Dr.Web Enterprise Security Suite** and its components, ensure availability of your Internet connection.

Check that the Internet Protocol is properly configured and DNS server settings are specified correctly.

The anti-virus software and virus databases can be updated either manually or through the schedule of a **Server** or an **Agent**.

Before updating the anti-virus software and virus databases you should set the configuration of the repository (including access to **Dr.Web Global Update System** as described in **Administrator Manual**, p. Editing the Configuration of the Repository).

8.1. Updating Dr.Web Server and Restoring from the Backup

Control Center provides the following features for managing **Dr.Web Server** software:

- Update the **Server** software to one of the available versions downloaded from the **GUS** and stored in the **Server** repository. Description of settings for updating the repository from **GUS**, is given in the Administration of Dr.Web Server Repository section.
- Rollback the **Server** software to the saved backup. The **Server** backups are created automatically during update to the new version in the **Dr.Web Server Updates** section (step 4 in the procedure below).

Upgrading the **Server** within version **10** can be also performed via the **Server** distribution kit. The procedure is described in the **Installation Manual**, in the Upgrading Dr.Web Server for Windows® OS or Upgrading Dr.Web Server for UNIX® System-Based OS sections.

Not all **Server** updates within version **10** have the distribution kit file. Some of them can be installed via the **Control Center** only.

After the **Server** upgrade under UNIX system-based OS via the **Control Center**, the **Server** version in the OS package manager will not be changed.

To manage Dr.Web Server software:

1. Select the **Administrating** item in the main menu of the **Control Center**, in the opened window, select **Dr.Web Server** in the control menu.
2. To open the **Server** versions list, perform one of the following actions:
   - Click the current version of the **Server** in the main window.
   - Click **Versions list**.
3. This opens the **Dr.Web Server Updates** section with the list of available updates and backups of the **Server**. At this:
   - The **Current version** list contains the version of the **Server**, used at the moment. The **Change list** section contains the brief list of new features and the list of errors which had been resolved in this version relatively to the previous updates version.

- The **All versions** list contains the list of this **Server** updates downloaded from **GUS**. The **Change list** section contains the brief list of new features the list of errors which had been resolved in each update.

For the version that corresponds to the first installation of the **Server** from the installation package, in the **Change list** is empty.

- The **Backups** list contains the list of backup copies which are stored for this **Server**. The **Date** section contains the information on the date of the back up.

4. To update the **Server** software, set the option next to the necessary version of the **Server** in the **All versions** list and click **Save**.

You can update only to a later version of the **Server** regarding to the currently used version.

During the **Server** update, the current version is saved as a backup (placed to the **Backups** section), and version to which update is performed, is moved from the **All versions** to the **Current version** section.

Backup copies are saved in the following folder:

`var` → `update_backup_`*<old_version>*`_`*<new_version>*

During update, the `var` → `dwupdater.log` log file is created or supplemented.

5. To rollback the **Server** software to the saved backup copy, set the option next to the necessary version of the **Server** in the **Backups** list and click **Save**.

During the **Server** software rollback, the applied backup copy is placed to the **Current version** section.

8.2. Manual Updating of Dr.Web Enterprise Security Suite Components

Checking for Updates from GUS

To check for updates of Dr.Web Enterprise Security Suite products on the updates server

1. Select the **Administration** item in the main menu and click **Repository state** in the control menu.
2. In the opened window information about all components are listed, also last revision date and its current state is specified. Click **Check for updates**.
3. If the checked component is outdated, it will be updated automatically during the check. Products are updated according to the settings of the repository (read p. Administration of Dr.Web Server Repository and further).

Updating the Software

To update the software of an anti-virus station through Dr.Web Security Control Center

1. Select the **Anti-virus network** item in the main menu, then click the name of the station or group in the hierarchical list.
2. In the toolbar, click **Components management**. In the opened submenu select the necessary forced update mode:
   - **Update failed components** instructs to reset the error state and update only those components that failed at the previous update;
   - **Update all components** instructs to force the update of all components, including those updated successfully.

After forced update of all components, reboot of a station is required. Follow the **Agent** instructions.

8.3. Scheduled Updates

You can make a schedule on a certain **Dr.Web Server** to regularly check for software updates and synchronize products in the repository with new versions on another **Dr.Web Server** or the **GUS** server.

For more details on the schedule, see p. Setting Dr.Web Server Schedule.

To schedule product updates on Dr.Web Server:

1. Select the **Administration** item in the main menu and click **Dr.Web Server Task Scheduler** in the control menu. The list with the current tasks of the **Server** will be opened.
2. To add a task, click **New task** in the toolbar.
3. In the opened window assign a name to the task in the **Name** field.
4. Go to the **Action** tab and select the **Update** action in the drop-down list.
5. In the opened list, set the flag next to those components which will be updated by this task.
6. Go to the **Time** tab and in the **Time** drop-down list, set the time span of running the task and specify time according to the time span selected.
7. Click **Save** to accept the changes.

8.4. Updating the Repository of a Server not Connected to the Internet

8.4.1. Copying Repository of Other Dr.Web Server

If the anti-virus **Server** is not connected to the Internet, its repository can be updated manually. Copy the repository of another **Dr.Web Server**, which has been updated normally.

This way is not meant for upgrading.

To update the anti-virus software, do the following:

1. Install the anti-virus **Server** software on another computer connected to the Internet as described in the **Installation Manual**, p. Installing Dr.Web Server.
2. Stop the two **Servers**.
3. Start the **Server** connected to the Internet with the syncrepository switch to update the anti-virus software.

   Example for **Windows** OS:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" syncrepository
   ```

4. Fully replace the content of repository catalog on the main (working) **Server** by the content of correspondent catalog of the **Server** connected to the Internet. Usually it is:
   - `var\repository` under **Windows** OS,
   - `/var/drwcs/repository` under **FreeBSD** OS,
   - `/var/opt/drwcs/repository` under **Linux** OS and **Solaris** OS.

If the **Agent** with an active self-protection is installed on **Sever** computer, you must disable **Dr.Web Self-protection** component in the **Agent** settings before starting the repository update.

5. If the main **Server** is runing under UNIX OS, it is necessary to set the rights of the user created/ selected at the installation of the **Server** to the copied repository.
6. On the main **Server** execute the command

   ```
   drwcsd rerepository
   ```

   Under **Windows** OS the command can be performed both from the *command line*:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" rerepository
   ```

   or from the *Start* menu:

   `Start → All Programs → Dr.Web Server → Server control → Reload repository`

7. Start the main **Server**.

If **Dr.Web Self-protection** component was disabled before the repository update, it is recommended to enable this component after updating.

8.4.2. Downloading Repository from GUS

If **Dr.Web Server** is not connected to the Internet, you can update its repository manually by importing the repository downloaded from **GUS**.

To download **Dr.Web Server** repository from **GUS**, use the **Dr.Web Repository Loader** standard utility.

Features of Use

- To download the repository from **GUS**, you need a license key of **Dr.Web Enterprise Security Suite** or its MD5 hash which you can view in the **Control Center** in the **Administration** → **License Manager** section.
- You can launch **Dr.Web Repository Loader** in the following modes:
  - graphical version of utility (under Windows OS only),
  - console version of utility.
- When downloading the repository from the **GUS**, a proxy server can be used.

8.4.2.1. GUI Utility

GUI version of **Dr.Web Repository Loader** utility can be downloaded via the **Control Center**, in the **Administration** → **Utilities** section. You can run this utility version on any computer under Windows OS with Internet access. Executable file is `drwreploader-gui-<version>.exe`.

To download repository via the GUI version of Dr.Web Repository Loader:

1. Run the GUI version of **Dr.Web Repository Loader** utility.
2. In the main window of the utility, specify the following parameters:
   a) **License key or MD5 of the key** - specify **Dr.Web** license key file. Click **Browse** and select active license key file. Instead of license key you can specify only MD5 hash of the license key, which you can view in the **Control Center** in the **Administration** → **License Manager** section.
   b) **Downloading folder** - specify the folder to download repository to.
   c) In the **Mode** list, select on of the updates loading mode:
      - **Load repository** - repository is downloaded in the **Server** repository format. Loaded files can be directly imported via the **Control Center** as the **Server** repository updates.
      - **Synchronize update mirror** - repository is downloaded in the **GUS** updates zone format. Loaded files can be placed on the updates mirror in your local network. Further, **Servers** can be configures to receive updates directly from this updates mirror containing the last version of the repository but not from the **GUS** servers.
   d) Set the **Archive repository** flag to pack downloaded repository into zip archive automatically. This option allows to get prepared archive file for import downloaded repository archive to the **Server** via the **Control Center**, for the **Administrating** → Repository Content section.
3. If you want to change the additional settings for **GUS** connections and updates downloading, click **Additional settings**. In the opened settings window, the following tabs are available:
   a) On the **Products** tab, you can change the list of products to download. In the opened settings window, the list of all repository available for downloading for the **GUS** is presented:
      - To update the list of products currently available on the **GUS**, click **Update**.
      - Set the flags next to whose products that you want to download from the **GUS** or the flag in the head of the table to select all products from the list.
   b) On the **Dr.Web GUS** tab, you can configure update servers parameters:

- **GUS** servers are listed in the order the utility contacts them when downloading the repository. To change **GUS** server order, use the **Up** and **Down** buttons.
- To add a **GUS** server to the list of servers used for updates, specify the address of the **GUS** server under the servers list and click **Add**.
- To remove a **GUS** server from the list of used, select the server you want to delete and click **Remove**.
- In the **Base URI** field, specify a **GUS** servers folder where updates of **Dr.Web** products are located.
- In the **Protocol** drop-down list, select the protocol type to receive updates from update servers. For all protocols, updates are downloaded according to the settings of the **GUS** servers list.
- In the **Allowed certificates** drop-down list, select the type of SSL certificates that will be automatically accepted. This option is used only for secure protocols that support encrypting.
- **Login** and **Password** - user credentials to authenticate on updates server, if the updates server requires authorization.
- Set the **Use CDN** flag to allow downloading repository from GUS via Content Delivery Network.

c) On the **Proxy Server** tab, you can specify parameters for connecting ti the **GUS** via the proxy server:
- **Proxy server address** and **Port** - the network address and the port number of the proxy server to use correspondingly.
- **Login** and **Password** - authorization parameters on the proxy server if used proxy server requests authorization.

d) On the **Scheduler** tab, you can configure the schedule to receive updates periodically. To execute the schedule, the Task schedule of Windows OS is used. At this, you do not have to launch the utility manually, the repository downloading performed automatically according to the specified time slots.

e) On the **Log** tab, you can configure parameters of updates downloading log.

Click **OK** to apply specified changes and to return to the main widow of **Dr.Web Repository Loader**.

4. After configuring all parameters, click **Download** in the main window of **Dr.Web Repository Loader** to start connecting to the **GUS** and downloading the repository.

8.4.2.2. Console Utility

Console version of **Dr.Web Repository Loader** utility is located in the `bin` subfolder of **Dr.Web Server** installation folder. You are allowed to run this utility version only from this **Server** folder. Executable file is `drwreploader`.

Available Download Methods

Recommended procedure

1. Download the **Server** repository from **GUS** using the `drwreploader.exe` utility. When downloading, use the `--archive` switch to archive the repository.
2. Import the downloaded repository to **Server** via the **Control Center**, from the **Administration** → Repository Content section.

Manual import

1. Download the **Server** repository from **GUS** using the `drwreploader.exe` utility without the `--archive` switch. When downloading, use the `--path` <*argument*> switch to download the repository to the specified folder.
2. To import the repository, copy and replace files from the <*argument*> folder to the `/repository` folder in the **Server** installation folder.
3. Reload the repository from the **Control Center**, the **Administration** → Repository state section.

Possible Switches

- `--help` – show help message on switches.
- `--show-products` – show the list of **GUS** products.
- `--path` <*argument*> – download the repository from **GUS** to the folder specified as <*argument*>.
- `--etc` <*argument*> – path to the `etc` **Server** folder (used to search root certificates and update public keys).
- `--archive` – archive the repository.
- `--key` <*argument*> – path to the license key file (the key file or its MD5 hash must be specified).
- `--key-md5` <*argument*> – MD5 hash of the license key (the key file or its MD5 hash must be specified).
- `--product` <*argument*> – updated product. By default, entire repository is downloaded.
- `--only-bases` – download only virus bases.
- `--update-url` <*argument*> – **GUS** servers folder where updates of **Dr.Web** products are located (it is recommended to leave default value).
- `--servers` <*argument*> – **GUS** servers addresses (it is recommended to leave default value).
- `--prohibit-cdn` – deny CDN usage when downloading updates (by default is off, i.e. CND is used).
- `--prohibit-ssl` – use insecure HTTP instead of HTTPS (by default is off, i.e. HTTPS is used).
- `--cert-mode` [<*argument*>] – automatically accept HTTPS certificates.

  The <*argument*> may take one of the following values:

  - `any` – accept all certificates,
  - `valid` – accept only valid certificates,
  - `drweb` – accept only **Dr.Web** certificates.

The `drweb` value is used by default.

- `--proxy-host <argument>` – proxy server specified in the following format: *<server>*`[:`*<port>*`]`.
- `--proxy-auth <argument>` – data for authentication on the proxy server: user login and password *<login>*`[:`*<password>*`]`.
- `--strict` – terminate downloading if an error occurred.
- `--log <argument>` – create a log file of the **Server** log file format to register information on the downloading process and located it in the folder specified as *<argument>*.

Examples of Use

1. To create an imported archive with all products:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb Server\etc"
```

2. To create an imported archive with virus bases:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program Files\DrWeb Server
\etc"
```

3. To create an imported archive with **Server** only:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:\Program Files\DrWeb
Server\etc"
```

8.5. Update Restrictions for Workstations

Via **Dr.Web Security Control Center** you can configure update mode for **Dr.Web Enterprise Security Suite** at protected workstations in particular time slots.

To configure station update mode, perform the following actions:

1. Select the **Anti-virus network** item in the main menu, in the opened window click the name of a station or group in the hierarchical list. Select **Update restrictions** in the control menu.
2. In the **Update restriction** drop-down list, select the limitation mode:
   - **No restrictions** - do not restrict distribution of updates on stations.
   - **Forbid all updates** - forbid distribution of all updates on stations during time slots that are specified in the **Stations update timetable** table below.
   - **Update only bases** - forbid distribution of updates only for program modules during time slots that are specified in the **Stations update timetable** table below. Virus bases updates will be performed with no changes in a normal mode.
3. Set the **Limit updates traffic** flag to limit the network traffic amount during transmitting of updates between **Server** and **Agents**. In the **Maximal transmission speed (KB/s)** field, specify the value of maximal speed for updates transmission.

   For more details see Update Traffic Limitations.

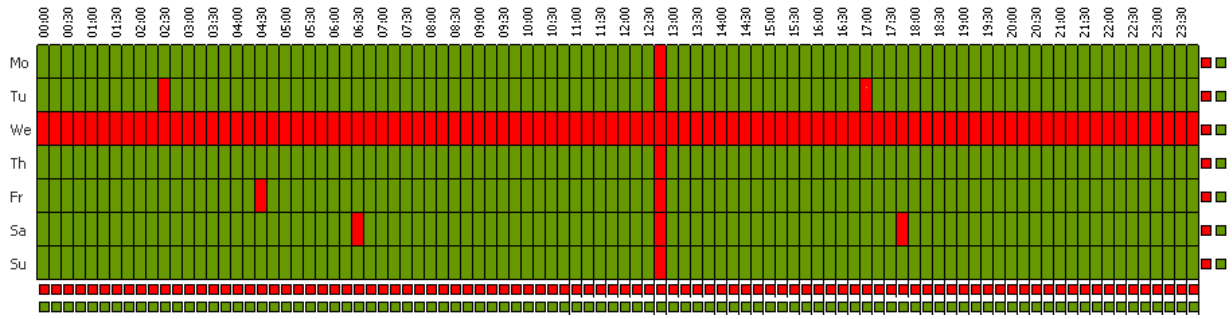
4. Set the **Receive all the latest updates** flag to transmit all components updates to the stations not depending on the limitations that are specified in the Detailed Repository Configuration section.

   If the flag is cleared, station receives only those updates which are marked as current updates for distribution.

5. In the **Stations update timetable** table, the update mode is specified using the following colors:
   - green - update is enabled,

■ red - update is disabled.

The restrictions are set separately for each 15 minutes of each day of the week.



To change the update mode, click the corresponding block of the table:

- To change the update mode for a row (full day), click the corresponding color in the right part of the table row.
- To change the update mode for a column (a particular 15 minutes interval of each day of the week), click the corresponding color under the table column.

6. After editing, click **Save** to accept changes.

In the toolbar, the following options are available:

Reset all parameters to initial values - restore the values that all parameters in this section had before current editing (last saved values).

Reset all parameters to default values - restore default values of all parameters in this section.

Propagate these settings to another object - copy settings from this section to settings of other station, group or several groups and workstations.

Set inheritance of settings from primary group - remove personal settings of a station and set inheritance of settings in this section from a primary group.

Copy settings from primary group and set them as a personal - copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered as a personal.

Export settings from this section to the file - save all settings from this section to a file of a special format.

Import settings to this section from the file - replace all settings in this section with settings from the file of a special format.

8.6. Updating Mobile Dr.Web Agents

If user's computer, laptop or mobile device has no connection to **Dr.Web Server** for a long time, to receive updates opportunely from the **Dr.Web GUS**, it is recommended to set the **Agent** mobile mode of operation on the station.

In the mobile mode the **Agent** tries to connect to the **Server** three times and, if unsuccessful, performs an HTTP update. The **Agent** tries continuously to find the **Server** at interval of about a minute.

The mobile mode will be available in the **Agent** settings if the mobile mode of using **Dr.Web GUS** has been allowed in the station permissions (for more, read p. Permissions of Station Users).

When the **Agent** is functioning in the mobile mode, the **Agent** is not connected to **Dr.Web Server**. All changes made for this workstation at the **Server**, will take effect once the **Agent** mobile mode is switched off and the connection with the **Server** is re-established.

In the mobile mode only virus databases are updated.

Description of mobile mode configuration at the **Agent** side is given in the **User Manual**.

Chapter 9: Configuring the Additional Components

9.1. Proxy Server

The anti-virus network may consist of one or several **Proxy servers**.

The main function of a **Proxy server** is to establish a connection between **Dr.Web Server** and **Dr.Web Agents** in cases when it is impossible to set up direct access (e.g. if **Dr.Web Server** and **Dr.Web Agents** are located in separate networks which do not have packet routing between them).

To establish a connection between the **Server** and clients via the **Proxy server**, it is recommended to disable traffic encryption. For this, it is enough to set the **no** value for the **Encryption** parameter in the Dr.Web Server Configuration > General section.

General Functions

A proxy server performs the following functions:

1. Network listening and receipt of connections according to the specified protocol and port.
2. Protocol translation (supported protocols: TCP/IP).
3. Data transmission between **Dr.Web Server** and **Dr.Web Agents** according to the **Proxy server** settings.
4. Caching of **Agent** and anti-virus package updates, which are translated by the **Server**. In case of using cache of the **Proxy server** to translate updates, following are provided:
   - reducing of network traffic,
   - reducing of **Agent** updates receiving time.

Proxy servers can be composed to hierarchical structure.

The general diagram of the anti-virus network when a **Proxy server** is used is illustrated in the figure 9-1.

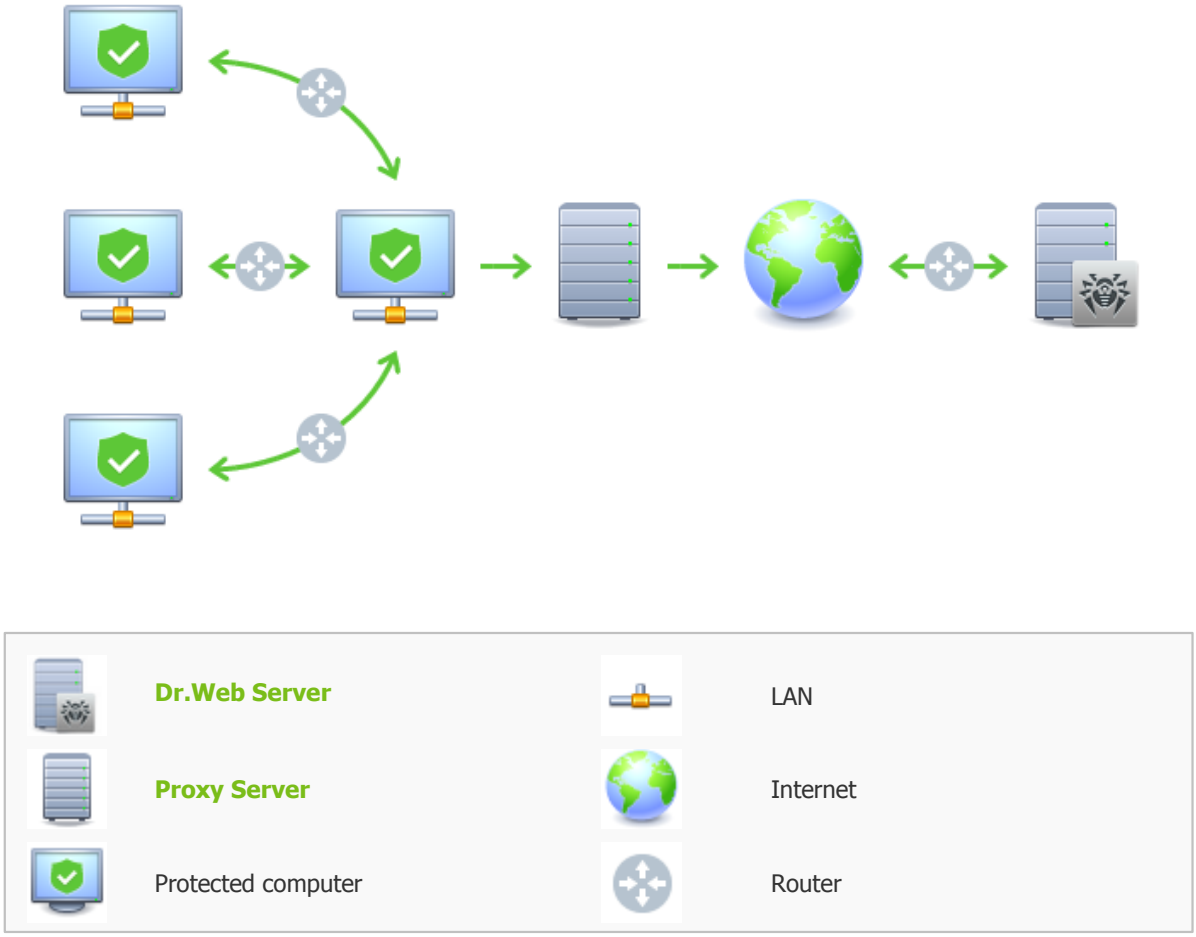


Figure 9-1. Diagram of the anti-virus network when a proxy server is used

Principle of Operation

When a proxy server is used, the following operations are performed

1. If the address of the **Server** is not specified on the **Agent**, the **Agent** sends a multicast request according to the protocol of the network.
2. If the **Proxy server** is set up to translate connections (the `discovery="yes"` parameter), a message about the availability of an operating **Proxy server** is sent to the **Agent**.
3. The **Agent** sets the received **Proxy server** parameters for **Dr.Web Server**. Further intercommunication is performed transparently for the **Agent**.
4. The **Proxy server** listens specified ports for incoming connections via given protocols according to the configuration file.
5. For each incoming connection from the **Agent** (or **Dr.Web Server**) the **Proxy server** establishes a connection with **Dr.Web Server** (or **Agent**).

The forwarding algorithm for the list of Dr.Web Servers

1. **Proxy server** loads to RAM the list of **Dr.Web Servers** from the `drwcsd-proxy.xml` configuration file (see the **Appendices** document, p. Appendix G4).
2. **Dr.Web Agent** connects to the **Proxy server**.
3. **Proxy server** forwards **Dr.Web Agent** to the first **Server** from **Dr.Web Servers** list loaded in the RAM.

4. **Proxy server** rotate the list in the RAM and moves **Dr.Web Server** from the first position to the end of list.

Proxy Server does not save changed order of **Servers** to its configuration file. After restart of **Proxy server**, the list of **Dr.Web Servers** is loaded to the RAM in original version, which is stored in the configuration file.

5. When the next **Agent** connects to the **Proxy server**, procedure is repeated from the step 2.
6. If the **Dr.Web Server** disconnects from the anti-virus network (e.g., gets offline or denies of service), the **Agent** connects to the **Proxy server** repeatedly and procedure is repeated from the step 2.

Network scanner which is launched from an external network (in respect to the **Agents**) is unable to locate the installed **Agents**.

If the **Replace NetBios names** flag is set and anti-virus network contains the **Proxy server**, when for all stations connected to the **Server** via the **Proxy server**, in **Dr.Web Security Control Center**, the name of computer on which the **Proxy server** is installed, will be shown instead of stations names.

Traffic Encryption and Compression

Proxy server supports traffic compression. Transferred data is processed regardless of whether traffic is compressed or not.

Proxy server does not support traffic encryption. It analyzes transferred data and if traffic between **Dr.Web Server** and **Agent** is encrypted, **Proxy server** switches to the transparent mode, i.e. transfers all traffic between **Server** and **Agent** without any data analyzing.

If encryption between **Server** and **Agent** is enabled, **Proxy server** do not caching updates.

Caching

Proxy server supports traffic caching.

Products are cached by revisions. Each revision stores in separate directory. Directories with all next revisions contain *hard links* on existing files from old revisions and originals for changed files. Thus, files for each version are stored on a hard drive in a single exemplar, all directories for next revisions contain only links on unchanged files.

According to the settings specified in the configuration file, the following actions are performed if the caching is enabled:

- Outdated revisions are periodically deleted. By default - once per hour.
- Only latest revisions are stored. All other, earlier revisions are considered outdated and are deleted. By default 3 last revisions are stored.
- Unused *memory mapped* files are periodically unloaded. By default - each 10 minutes.

Settings

The **Proxy server** does not have a GUI. Its settings are adjusted via a configuration file. The format of the configuration file is described in the **Appendices** document, p. Appendix G4.

Only user with administrative rights on the computer can manage settings (edit configuration file) of **Proxy server**.

For proper operation of **Proxy server** under Linux system-based OS after computer reboot, you must edit system network configuration without Network manager.

Starting and Stopping

To start and stop the **Proxy server** under Windows OS, open **Control Panel** → **Administration** → **Services**, then double-click `drwcsd-proxy` and select a necessary action in the opened window.

To start and stop the **Proxy server** under a UNIX-based OS, use the `start` and `stop` commands with scripts created during installation of the **Proxy server** (see the **Installation Manual**, p. Installing Proxy Server).

To start the **Proxy-server** under both Windows OS and UNIX system-based OS, you can run the `drwcsd-proxy` executable file with corresponding switches (see the **Appendices** document, p. H8. Proxy Server).

9.2. NAP Validator

Overview

Microsoft® Network Access Protection (NAP) is a policy enforcement platform built into Windows OS that allows you to better protect network assets by enforcing compliance with system health requirements.

With NAP, you can create customized health requirement policies to validate computer health in the following cases:

- before allowing access or communication,
- automatically update compliant computers to ensure ongoing compliance,
- optionally confine noncompliant computers to a restricted network until they become compliant.

Detailed description of NAP technology is given on Microsoft company web site.

NAP in Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite allows you to use the NAP technology to check health of **Dr.Web** anti-virus software on protected workstations. This functionality is provided by use of **Dr.Web NAP Validator**.

Means of Health Validation

- A NAP health policy server which is installed and configured in the network.
- **Dr.Web NAP Validator** which is an implementation of NAP System Help Validator (SHV) with use of **Dr.Web** custom policies extensions. This component is installed on the computer where the NAP server resides.
- System Health Agents (SHAs) which are installed automatically on the workstations during installation of **Dr.Web Agents**.
- **Dr.Web Server** which serves as the NAP remediation server and ensures health of anti-virus software on workstations.

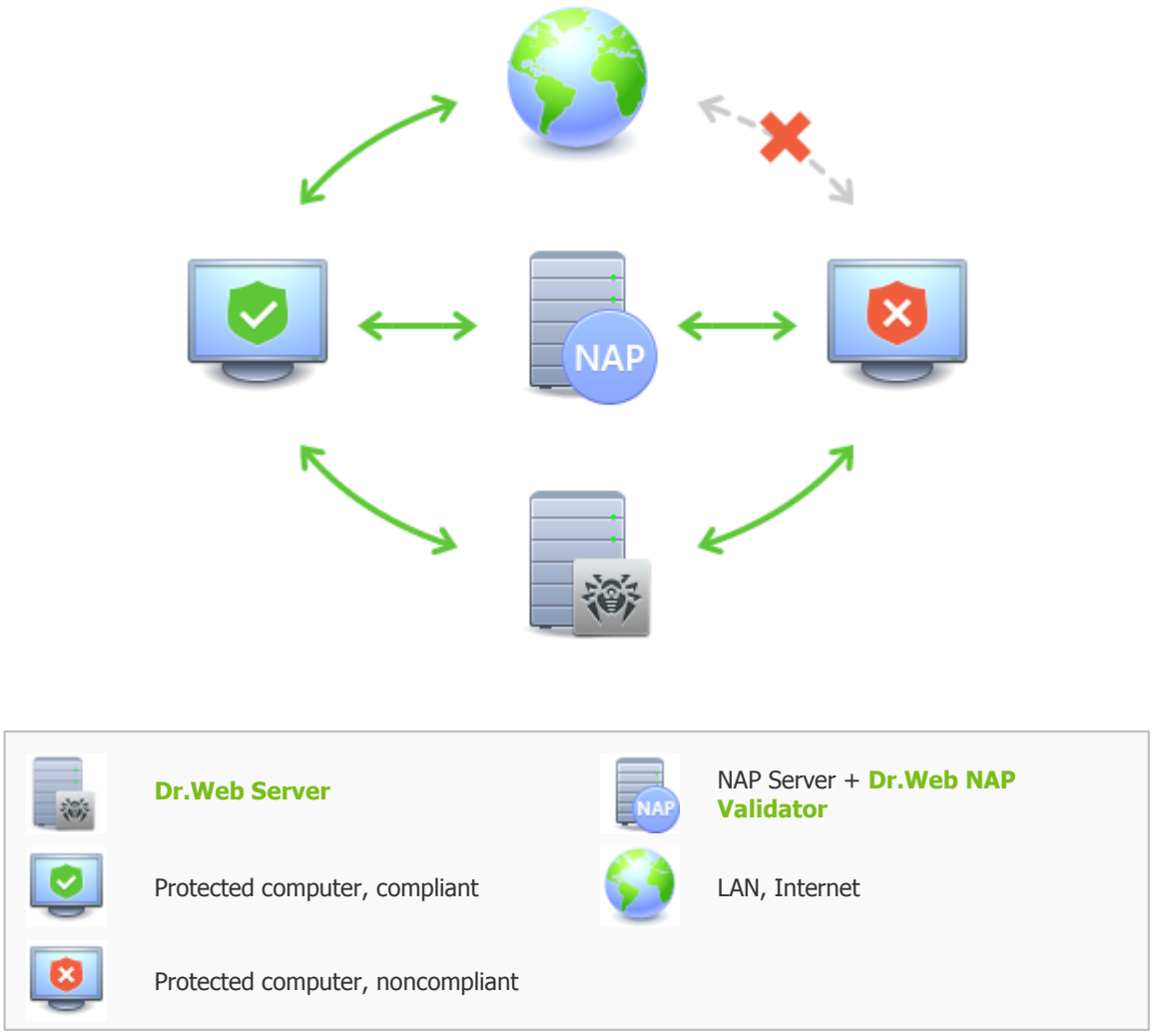


Figure 9-2. Diagram of the anti-virus network when NAP is used

Workstation Validation Procedure

1. Validation is activated when you configure the corresponding settings of the **Agent**. For more information, see Managing Dr.Web Agent for Windows® OS.
2. The SHA connect to **Dr.Web NAP Validator** installed on the NAP server.
3. **Dr.Web NAP Validator** determines compliance of workstations against the health requirement policies as described below. To determine health compliance, **NAP Validator** checks workstation anti-virus state against the corresponding health requirement policies, and then classifies the workstation in one of the following ways:
   - Workstations which meet the health policy requirements are classified as compliant and allowed unlimited access and communication on the network.
   - Workstations which do not meet at least one requirement of the health policy are classified as noncompliant and have their access limited to **Dr.Web Server** only. The **Server** allows noncompliant workstations to update the system with the necessary anti-virus settings. After update, the workstations are validated again.

Health Policy Requirements

1. **Dr.Web Agent** must be started and running (**Agent** health).
2. **Dr.Web** virus databases must be up-to-date, i.e. databases on the workstation must be similar to those on the **Server**.

Configuring NAP Validator

After installation of **Dr.Web NAP Validator** (see **Installation Manual**, p. Installing NAP Validator) on a computer where a NAP server resides, you need to perform the following actions:

1. To open NAP server configuration component, run the `nps.msc` command.
2. In the **Policies** section, select **Health Policies**.
3. In the opened window, open properties of the following elements:
   - **NAP DHCP Compliant**. In the settings windows, set the **Dr.Web System Health Validator** flag which prescribes to use **Dr.Web NAP Validator** component policies. To classify workstations as compliant only when all health policy requirements are met, select **Client passed all SHV checks** in the drop-down list.
   - **NAP DHCP Noncompliant**. n the settings windows, set the **Dr.Web System Health Validator** flag which prescribes to use **Dr.Web NAP Validator** component policies. To classify workstations as noncompliant if any of the health policy requirements are not met, select **Client failed one or more SHV checks** in the drop-down list.

Index

A

accounts 66
Administrators
  permissions 66
Agent
  functions 29
  interface 29
  mobile mode 189
  settings 100
  updating 189
alerts
  settings 153
anti-virus network 171
  components 54
  setting connections 173
  structure 54, 171
  updating 177
  virus events 177
anti-virus Scaner 106
anti-virus scanning 106
anti-virus Server
  interface 25, 27
  log 24
  logging 125
  schedule 141
  setting connections 173
  settings 127
  start 26, 29
  tasks 24
  types of connections 171
approving stations 83
authorization, Control Center 43
automatic authorization 43

C

components
  anti-virus network 54
  synchronization 183
connections, between the Servers
  setting 173
  types 171
Control Center
  description 30
  hierarchical list 35
  main menu 31
  property pane 39
  toolbar 36
creating
  groups 75

D

demo key files 23
distribution kit 21
Dr.Web Server
  start 29
Dr.Web Agent
  functions 29
  interface 29
  mobile mode 189
  settings 100
  updating 189
Dr.Web Server
  installation folder structure 25, 27
  interface 25, 27
  log 24
  logging 125
  schedule 141
  setting connections 173
  settings 127
  start 26
  tasks 24
  types of connections 171

E

encryption
  traffic 129

F

force update 183
functions
  Agent 29
  anti-virus Server 24

G

groups 73
  adding a station 77
  configuration, inheriting 80
  primary 80
  removing a station 77
  settings 80
  settings, propagation 82

Index

GUS
see also manual updating 183

I

icons
hierarchical list 35, 151
network scanner 46
interface
Agent 29
anti-virus server 25, 27

K

key files 22
demo 23
receiving 22
see also registration 22

L

language
Control Center 41, 68
licensing 22

M

manual updating 183
mobile mode of the Agent 189

N

NAP Validator 194
setting 196
Network Scanner 45
newbie 83, 100
notifications
repository, updating 159
sending, to the users 121

P

permissions
Administrators 66
users 91
preinstalled groups 73
primary groups 80
proxy server
functionality 191
start, stop 194

R

registration
Dr.Web product 22
stations, at the Server 83
removing
groups 75
stations, from a group 77
repository
simple editor 160
Repository Loader 185
rights
Administrators 66
users 91

S

Scanner
anti-virus 106
Network 45
scanning
automatic 92
manually 106
schedule
Server 141
updates 183
Server logging 125
settings
Agent 100
anti-virus Server 127
propagation 82
start
Dr.Web Server 26, 29
station
adding to a group 77
administration 83
approving 83
configuration, inheriting 80
newbie 83, 100
removing from a group 77
scanning 92, 106
settings, propagation 82
statistics 114
unapproved 83
statistics
station 114
synchronization

Index

synchronization
components 183
system requirements 17

T

traffic
composition 55
compression 129
encryption 129

U

unapproved stations 83
update
restrictions 188
update restrictions 188
updating
Agent 189
anti-virus network 177
Dr.Web ESS 181
force 183
manual 183
mobile mode 189
notifications 159
scheduled 183

© Doctor Web, 2015